TARTU ÜLIKOOL

Majandusteaduskond

Olev Gudovski

BIOMEETRILISTE MAKSETE RAKENDUSPERSPEKTIIVID EESTIS

Bakalaureusetöö

Juhendaja: dotsent Nadežda Ivanova

Tartu 2018

Soovitan suunata kaitsmisele……..

dotsent Nadežda Ivanova

Kaitsmisele lubatud…….2018.a.

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

……..

Olev Gudovski

SISUKORD

SISSEJUHATUS

Kiire tehnoloogiline areng, mis hõlmab erinevaid valdkondi on põhjus, miks ka maksemeetodite temaatikale peab pöörama suuremat tähelepanu. Maksete valdkond on suur, mitmekülgne ja kõikihõlmav. Igapäevaselt sooritatakse erinevates müügikohtades suures ulatuses tehinguid. Maksemeetodid ja nende eelistused müügikohtades on finantsteenuste kategooria osa. Finantsteenuste areng on omakorda sõltuvuses finantstehnoloogia (*FinTech*) sektorist, mis loob innovaatilisi finantslahendusi (Sokolowska 2015:292). Koos uudsete lahendustega areneb ka finantsteenuste turg, mis omakorda avaldab positiivset mõju majandusele.

Maksetehingu sooritamise kiirus, mugavus ja turvalisus on kolm põhilist näitajat, mis peavad pidevalt paranema. Kui see valdkond ei oleks püsivas arengus, siis kurjategijatel oleks lihtsam leiutada meetodeid, kuidas saaks kuritarvitada võõraid maksevahendeid. Maksevõimaluste areng elavdab konkurentsi panganduse ja *FinTech´*i sektorite lõikes ning suudab luua eelise neile, kes lähevad arenguprotsessiga kaasa.

Käesoleva töö autori arvates võiksid järgmiseks võimalikuks sammuks maksemeetodite arengus olla biomeetrilised maksed, millele on viimasel ajal suurt tähelepanu osutanud tuntumad autoriseerimisvõrgud viies läbi erinevaid uuringuid ja luues vajalikke spetsifikatsioone biomeetrilise autentimise protsessi seisukohast (Mastercard and Visa…2018). Töö aktuaalsus ja unikaalsus seisneb selles, et fookuses on Eestis kasutusel olevad maksemeetodid ja koos sellega ka potentsiaalsed arengusuunad, milleks antud juhul on biomeetrilised maksed ning kokkuvõttes on tegemist innovatiivse teemaga. Avalikult pole Eestis seda valdkonda uuritud. Võiks oletada, et selle põhjused on seotud selliste mõistetega nagu ärisaladus, ettevõtete äristrateegia jms. Biomeetrilisi makseid on varasemalt uuritud kui makse kinnitamise vahendit. Tõepoolest, rääkides biomeetrilisest maksest, peetakse eelkõige silmas biomeetrilist

autentimist, mis antud kontekstis tähendaks makse kinnitamist, kasutades selleks biomeetrilist meetodit, mis asendaks tavapäraseid meetodeid, milleks on näiteks PIN-kood või salasõna sisestus vastavalt müügikoha tüübile. Kogu meetodi eelis peitub selles, et autentimise meetod on alati inimesega kaasas, sest inimene ongi andmekandja, mille tulemusena ei pea midagi kaasas kandma või meeles pidama.

Tehingute sooritamiseks müügikohtades saab kasutada sularaha ja pangakaarti või selle baasil töötavaid lahendusi nagu näiteks teatud liiki e-rahakotte ja Internetis ostlemiseks mõeldud makseteenuste pakkujate platvorme. Kaardimaksed on uudsete ja kaasaegsete maksemeetodite fundamentaalseks aluseks. Tegemist on turvalise ja kiire maksemeetodiga võrreldes sularaha kasutusega (Korolev, Krivosheya 2017:2). Biomeetrilise lahenduse sidumine kaardimakseloogikaga on üks võimalikest lähenemisest valdkonna arendamiseks kuna selline lähenemine teeb makseptosessi veelgi mugavamaks, turvalisemaks ja kiiremaks. Teisest küljest, saab teoreetiliselt käsitleda ka biomeetrilist meetodit, mille puhul ei oleks lisavahendite kasutamine vajalik ehk tehingu teostamiseks piisaks vaid biomeetriliste andmete lugemisest, mida saaks nimetada ka otseseks biomeetriliseks makseks.

Toetudes eespool mainitud argumentidele, keskendub käesoleva töö autor biomeetrilise autentimise temaatikale ja müügikohtades tehingute sooritamise võimalustele, mis toimuvad kaardimakse baasil ning nende võimalikule omavahelisele integratsioonile.

Biomeetriliste maksete rakendusperspektiive saab uurida erinevate sidusrühmade vaatenurgast. Nendeks on autoriseerimisvõrgud, pangad, finantstehnoloogia ettevõtted, riik, jaemüügi ettevõtted ja eraisikud. Terviklikku ülevaadet on võimalik saavutada uurides antud teemat mitmekülgselt. Kuna iga lahendus on mõeldud lõppkasutaja jaoks, siis selle tulemusena käesolev töö keskendub eelkõige eraisikutest tarbijatele. Inimeste avatus uudsete meetodite vastuvõtmiseks on oluline faktor, mis mängib suurt rolli innovatiivsete ideede ja nendega kaasnevate makselahenduste jätkusuutlikkusele.

Töö eesmärk on välja selgitada potentsiaalsete tarbijate huvi biomeetriliste maksete suhtes Eestis. Eesmärgi saavutamiseks on püstitatud järgmised uurimisülesanded:

- käsitleda biomeetrilise autentimise olemust ja selle sobilikke meetodeid maksetes kasutamiseks,
- käsitleda hetkel müügikohtades kasutatavate maksemeetodite sisu ja toimimisloogikat toetudes teaduskirjandusele,
- anda teaduskirjanduse põhjal ülevaade võimalikust biomeetriliste meetodite integreerimisest kasutuses olevate maksemeetoditega
- anda toetudes biomeetrilise autentimise ja teadaolevate maksemeetodite toimismehhanismi käsitlustele ülevaade biomeetrilise makse olemusest,
- lähtudes teoreetilisest käsitlusest ja varasematest empiirilistest uuringutest koostada ankeet ning viia läbi küsitlus eraisikutest maksjate hulgas,
- analüüsida saadud tulemusi ja teha järeldusi koos autoripoolse hinnanguga biomeetrilise maksemeetodite rakendamise ja arendamise osas

Lähtudes püstitatud eesmärgist ja uurimisülesannetest on bakalaureusetöö jagatud kaheks osaks. Teoreetilises osa esimeses alapeatükis on käsitletud biomeetrilise autentimise olemust, mis omakorda sisaldab kahe põhilise tuvastusprotsessi süsteemi käsitlust ning nende funktsioneerimise loogikat. Samuti on välja toodud erinevad biomeetriliste andmete kandjad, millelt saab lugeda andmeid ning lähtudes teaduskirjandusest on välja valitud enam sobilikumad võimalused maksete teostamiseks. Teoreetilise osa teises alapeatükis on käsitletud toetudes erinevatele teadusartiklitele tänapäeval müügikohtades kasutusel olevaid maksemeetodeid ning nende toimimist, mis omakorda toetuvad kaardimakse loogikale. Teine teoreetiline alapeatükk on omakorda seoses esimesega kuna tavapärased maksemeetodeid vaadeldakse läbi integratsiooniperspektiivi biomeetriliste autentimise süsteemide lõikes.

Töö empiiriline osa on jagatud kaheks alapeatükiks. Esimeses alapeatükis on käsitletud varasemad empiirilised uuringud, mis käsitlevad mitmekülgselt antud teemat. See sisaldab valitud autentimisviiside täpsuse uuringuid, maksete autoriseerimisvõrkude ja asjaosaliste organisatsioonide uuringuid ja seisukohti, aspekte millega peab arvestama empiirilise uuringu meetodi valimisel, erinevaid käsitlusi maksemeetodite lõikes ning

on tutvustatud autoripoolne metodoloogia uuringu läbiviimiseks, mis võtab arvesse nii teoreetilisi käsitlusi kui ka varasemaid empiirilisi uuringuid. Empiirilise osa teises alapeatükis on presenteeritud autoripoolse uuringu tulemused ja järeldused.

Töö on väärtuslik mõistmiseks, millele tuginedes saaks luua makselahendust, mis kasutab biomeetrilist autentimist. Antud tööd saaks kasutada alusena spetsiifilisemate uuringute läbiviimiseks rakendates teisi uurimismeetodeid ning piiritledes teemat vastavalt vajadusele. Kindlasti pakuks antud töö huvi erinevatele institutsioonidele, millest võiks tulla idee, kuidas kõik ära korraldada või hoopiski vastupidi, miks hoiduda selle kasutuselevõtust. Biomeetriliste maksete rakendamine võiks olla potentsiaalsete tarbijate huvides, sest korrektselt läbimõeldud ja välja töötatud lahendus võib olla mugavam ja kiirem. Esimesed makselahendused biomeetrilise autentimise toega, mis on kas juba olemas või on lähitulevikus turule tulemas, arvestades nende ülesehitust on turvalisemad ja turvalised ostud on kõikide osapoolte huvides. Finantsinstitutsioonidele pakuks mõtteainet, kas lähtudes klientide soovist, oleks tegemist pankade atraktiivse kasumlikku lahendusega või hoopiski võtaks mõne tuluallika vähemaks. Kui lahendus põhineb verifitseerimise süsteemil, mis toimib tuginedes kaardimakseloogikale, siis erilisi muutusi see endaga kaasa ei too. Kui aga leitakse töötav viis, kuidas käivitada otseseid biomeetrilisi makseid, mis ei eelda lisavahendite olemasolu, siis see võib endaga kaasa suuri muutusi maksete vastuvõtmise turul.

Tööd iseloomustavad märksõnad- biomeetriline autentimine, biomeetriline verifitseerimise ja identifitseerimise süsteem, maksemeetodid, kaardimakse, füüsiline müügikoht, e-kaubandus, mobiilimakse.

1. BIOMEETRILISE MAKSE TEOREETILISED ASPEKTID

1.1 BIOMEETRILISE AUTENTIMISE MEETODID

Biomeetrilise makse, kui mõiste vaatlemist, saab käsitleda mitmel erineval viisil. Ühest küljest on tegemist maksega, mille kinnitamiseks kasutab indiviid enda autentimiseks oma biomeetrilisi andmeid. Teisest küljest on teoreetiliselt võimalik käsitleda antud teemat vaatenurgast, mille kohaselt ei vaja indiviid eduka makse sooritamiseks lisavahedeid, peale oma biomeetriliste andmete, mida saaks nimetada ka otseseks biomeetriliseks makseks. Antud alapeatükis käesoleva töö autor käsitleb biomeetrilise autentimisega seotud definitsioone; autorite teoreetilisi seisukohti; erinevaid biomeetrilisi mõõtmisobjekte selgitamaks välja, millised andmekandjad on sobilikumad maksete konteksti ning käsitleb kaks põhilist biomeetrilise autentimise süsteemi toimimise loogikat, mida saaks integreerida kaardimakse toimimisloogikaga.

Biomeetria on üks võimalikest indiviidi tuvastusmeetoditest. Üldiselt on olemas kolm põhilist faktorit, mida tuvastussüsteemides kasutatakse (Normalini, Ramayah 2012:367) :

1. Midagi, mida kasutaja teab (parool, PIN);
2. Midagi, mida kasutaja omab (seade, kaart);
3. Midagi, mis kasutaja on (biomeetria)

Biomeetria on protsess, mida kasutatakse isiku autentimiseks või identifitseerimiseks, kasutades selleks füüsilisi või käitumuslikke karakteristikuid (Clodfelter: 2010:181). Kleist V.F (2007:319-329) on oma uuringutes jõudnud järeldusele, et biomeetrilised

autentimismeetodid kasvatavad kiiresti kasutajate seas usaldust ning omavad tugevat potentsiaali võrreldes traditsiooniliste autentimismeetoditega.

Wayman J.L. (2007:263-274) on oma teadusartiklis jõudnud järeldusele, et kõik mida hetkel peetakse biomeetrias uueks, oli arutlusel mitmeid aastaid tagasi ning ainus viis efektiivseks valdkonna arendamiseks peitub aru saamises, et ei ole otstarbekas uurida seda, mida on tehtud minevikus, vaid keskenduda tuleb tulevikule, arvestades käesoleva hetke tehnoloogilist arengut ja võimekust.

Tõepoolest saab Wayman´iga nõustuda, et käsitletavas valdkonnas ei ole põhitõed ajas muutuvad, kuid viisid, kuidas saab biomeetrilisi andmeid koguda ja töödelda on tugevas seoses tehnoloogilise arenguga kuna biomeetrilised andmekandjad ehk objektid, millelt saab neid andmeid lugeda ajas ei muutu.

Suure panuse biomeetria uurimisse on andnud Anil K. Jain, kelle teadustöödes on käsitlused aktuaalsed, hetkeolukorra ja võimalusi arvestavad ning seetõttu ka edasiviivad. Paljud autorid võtavad Anil Kumar Jain´i teadustöid oma uuringute aluseks.

Biomeetrilist autentimist on defineeritud kui järgmise generatsiooni tuvastusmeetodid, mis kasutab inimese biomeetrilisi parameetreid, mis on omakorda unikaalsed ning seetõttu ka usaldusväärsed (Breebaart *et al* 2011:606). Biomeetriline tuvastusmeetod on turvalisem seni teadaolevatest, sest maksevahendi tegelik omanik on koheselt teada (Coetzee 2013:73-75). Biomeetriline autentimine hõlmab endas indiviidi salvestatud biomeetriliste parameetrite mõõtmist ja võrdlemist. Biomeetrilise autentimise eesmärk on lugeda andmeid nende lugemise hetkel ning võrrelda neid varasemalt salvestatud andmetega. Kui traditsioonilised autentimismeetodid põhinevad millelgi, mida peab indiviid teadma või endaga kaasas kandma, siis biomeetrilise lähenemise puhul on tegemist tuvastamismeetodiga, mida kannab indiviid enda sees (Kim 1995:205–214).

Sisuliselt saab väita, et tegemist on sarnaste definitsioonidega. Biomeetrilise tuvastusmeetodi kannab iga inimene enda sees, aga füüsilise kaardi puhul on raske tuvastada, kas seda kasutav isik on maksevahendi ka reaalne omanik.

Tehnoloogia seisukohast saab biomeetrilist tuvastusprotsessi jagada kaheks süsteemiks, mis aitavad automaatselt kindlaks teha inimese identiteedi. Nendeks on verifitseerimise ja identifitseerimise süsteem. Verifitseerimise süsteemis indiviid esitab enda tuvastamiseks oma identiteedi süsteemile kontrolliks, kus viimane peale kontrollimistoimingute teostamist, kas kinnitab või lükkab tagasi esitatud andmed. Protseduuri edukaks teostamiseks peavad autentimist läbiva subjekti andmed olema sisestatud andmebaasi. Verifitseerimistoimingus saab protseduuri kirjeldada küsimusega: „Kas ma olen see, kes ma väidan, et olen?“. Identifitseerimise süsteem annab aga vastuse küsimusele: „Kas ma olen see, kes ma arvan, et olen?“. (Bolle *et al* 1997:1365)

Kaasaegsemates teadustöödes annavad autentimissüsteemide definitsioonid täpsema kirjelduse protseduuri toimimise kohta. On osutatud suurem tähelepanu protsessi toimise osas. Selle kohaselt, biomeetrilise identifitseerimise korral, võrreldakse konkreetse indiviidi loetud biomeetriliste parameetrite malli andmebaasis olevate varasemalt salvestatud mallidega. Toimingu hetkel süsteem täpselt ei tea, kellele vastavad andmed kuuluvad ja otsib mitme erineva malli hulgast, mis asuvad andmebaasis. Teisisõnu toimub „üks-mitmele“ vastavuse otsing ning andmebaas kontrollib, kas selline mall eksisteerib. Verifitseerimise süsteemis toimub „üks-ühele“ tuvastamine ehk biomeetrilise tuvastamisprotsessi hetkel toimub mallide vastavuse kontroll, mille korral süteem teab täpselt millist malli peab kontrollima. (Lumini, Nanni 2017:72)

Maksete kontekstis saab rakendada mõlemat tuvastusprotseduuri süsteemi. Kõik oleneb makselahenduse ülesehitatud arhitektuurist ning ka asjaolust, millisel etapil ning millistel tingimustel toimub biomeetriline tuvastus. Kui on tegemist makse kinnitusega, kus makse toimub tavapärast meetodit kasutades, milleks võib olla näiteks maksekaart või veebikeskkonnas registreeritud kasutajatunnus, siis on sobilik kasutusele võtta verifitseerimise süsteem. Kui aga makse saab alguse biomeetrilisest tuvastusest ning eelnevalt ei ole läbitud protseduuri, mis võiksid ennetavalt viidata konkreetsele isikule, siis selleks peab rakendama identifiseerimise süsteemi.

Olenemata sellest, kas tegemist on verifitseerimise või identifitseerimise süsteemiga, mõlemad jagavad ühist üldist andmevoogu ning koosnevad neljast põhikomponendist (Lumini, Nanni 2017:72):

1. Andmete vastuvõtu moodul. Esimene komponent süsteemis, mille ülesandeks on indiviidi biomeetriliste andmete lugemine. Olenevalt tuvastatavast objektist on riistvaraks kaamera, skänner või mikrofon. Sellel etappil on oluline, et kasutatakse kvaliteetset riist- ja tarkvara, kuna sellest oleneb terve süsteemi toimimine.

2. Andmete välja võtmise moodul. Selles faasis eemaldatakse saadud mallilt kõrvalekaldeid ja anomaaliaid. Seejärel leitakse üles unikaalsed parameetri väärtused, mida omakorda konverteeritakse tarkvara jaoks loetavale kujule. Kui andmed on töödeldud korrektselt, siis ei teki konverteerimisel vigu, mille tulemusena saab garanteerida, et arvesse on võetud just konkreetse indiviidi unikaalsed biomeetriliste parameetrite väärtused.

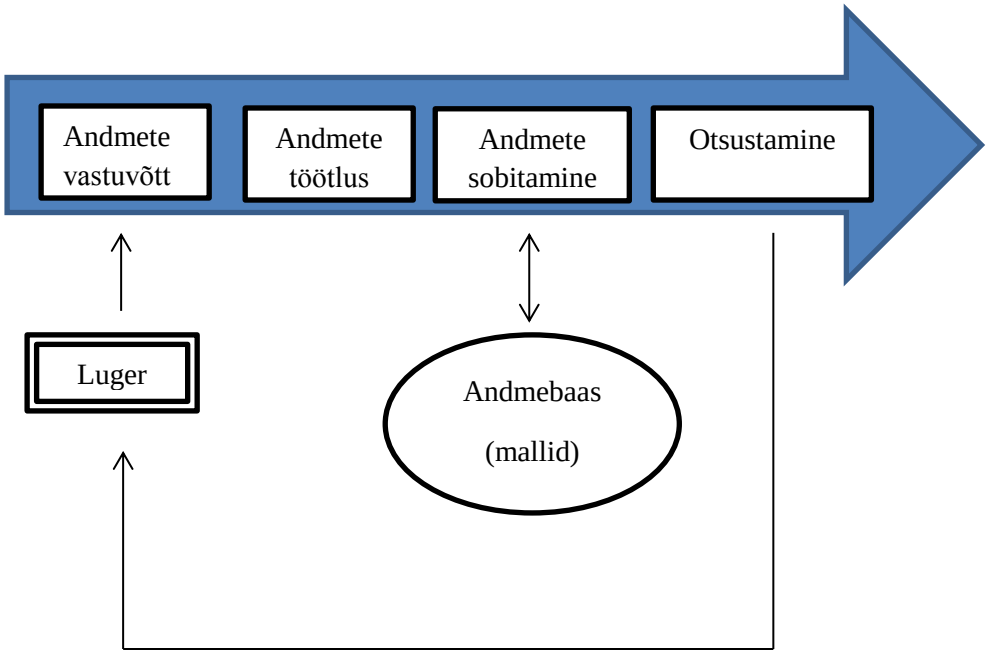
3. Andmete sobitamise moodul. Selles faasis andmebaas kontrollib või otsib saabunud töödeldud ja konverteeritud andmete sobivust baasis olevate eelsalvestatud andmetega. Näiteks sõrmejäljetehnoloogia tavapraktika puhul töötavad süsteemid sõrmejälje piltidega, millele on kantud kontrollpunktid, mis on omakorda fragmendid mustrist.

4. Otsustamise komponent. Viimane etapp, mis annab signaali, kas identifitseerimine või verifitseerimine on olnud edukas või mitte. Olenenevalt valdkonnast ja kehtestatud nõuetest, pannakse selles faasis paika biomeetrilise malli kontrollpunktide kattuvuse protsendi kriteerium.

Lumini ja Nanni loetletud nelja komponendi käsitlus annab hea ülevaate sellest, kuidas autentimise protsess peaks toimuma. Maksete kontekstis on tegemist indiviidi finantsvahenditega, mistõttu suurt tähelepanu peab osutama loetavate andmete kvaliteedile ning otsustamise komponendi faasis, peab olema biomeetrilise malli kattuvuse protsendi kriteerium kõrge ning andmebaasi suurenemisel kasvama veelgi.

Tuginedes identifitseerimis- ja verifitseerimissüsteemi käsitlusele, saab väita, et süsteemid omavad põhikomponentides ühist struktuuri, kuid väike erinevus

protseduurilistes aspektides siiski on, eriti makse sooritamise või kinnitamise vaatenurgast (vt joonis 1).

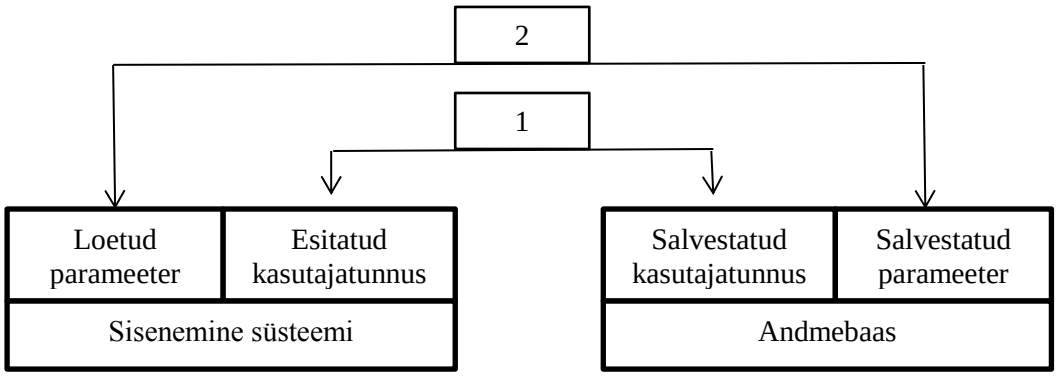


Joonis 1. Verifitseerimis- ja identifitseerimissüsteemi andmevoo protsess, autori koostatud (Lumini, Nanni 2017) põhjal.

Joonisel 1 on kujutatud verifitseerimis- ja identifitseerimissüsteemi andmevoo protsess. Protsess saab alguse süsteemi sisenemisest ning joonisel on kasutatud märksõnaks „luger“. Luger sobib rohkem kirjeldamaks identifitseerimissüsteemi, kuna sellisel juhul toimub päring andmebaasi, kus otsitakse esitatud malli koopiat kõikide mallide hulgast, mis on andmebaasis olemas. Verifitseerimissüsteemi puhul on tegemist pigem toimingu kinnitamisega kuna eelnevalt on toimunud mingi tegevus, mis annab süsteemile suuna edaspidise tuvastusprotsessi teostamiseks, seega üldistades sobib selline sõnapaar nagu „sisenemine süsteemi“.

Peale andmete saamist, peab seade olema võimeline võimalikult kvaliteetseid andmeid aktsepteerima. Seejärel toimub andmete töötlus, mille käigus elimineeritakse välistegurite mõju saadud parameetritele ning viiakse loetavale kujule. Sellele järgneb saadud parameetrite võrdlus andmebaasis olevate andmetega ning genereeritakse vastus. Positiivne või siis negatiivne vastus saadetakse tagasi seadmesse.

Põhiline parameetrite poolt läbitavate etappide üldine loogika on mõlema süsteemi puhul ühine. Verifitseerimise puhul on erinevus süsteemi sisenemise ja andmebaasi faasis (vt joonis 2).



Joonis 2. Verifitseerimissüsteemi loogika, autori koostatud (Lumini, Nanni 2017) alusel.

Joonisel 2 on välja toodud põhiline erinevus verifitseerimise ja identifitseerimise vahel. Verifitseerimisprotseduuris omab kasutaja enda tuvastamiseks lisavahendi, mida võib üldistatud kujul nimetada kasutajatunnuseks. Selleks võib olla mõni dokument, kaart, isiku konto vms. Kui kasutaja siseneb süsteemi, siis esitab ta lõpuks andmebaasile info, mis sisaldab kasutaja biomeetrilist objekti koos oma loetud biomeetriliste parameetritega. Andmebaas omalt poolt kontrollib, kas sellele kasutajatunnusele vastav biomeetriline parameeter on õige või mitte. Kokkuvõtvalt saab öelda, et kõigepealt toimub sobitamine kasutajatunnuse alusel ja teise etappina kontrollitakse ette antud kasutaja biomeetrilise objektiga seotud parameetrite kattuvust.

Teoreetiliselt saab iga indiviidi füsioloogilist või käitumuslikku tunnusjoont kasutada isiku tuvastamisprotseduuris. Järgnevalt on välja toodud nõuded, mis peavad olema täidetud nii teoreetilise kui ka praktilise käsitluse seisukohast (Bolle *et al* 1997:1365-1366).

Teoreetilised eeldused autentimisprotseduuri läbivale subjektile:

1. Universaalsus, mis tähendab, et igal indiviidil peab olema vajalik tunnus.

2. Unikaalsus, mis peab garanteerima, et erinevate indiviidide tunnused ei katu.

3. Püsivus, mis tähendab, et kindel tunnus aja jooksul ei muutu.

4. Kogumisvõime, mis tähendab, et tunnuseid saab mõõta kvantitatiivselt.

Praktilises käsitluses peavad olema täidetud järgmised kriteeriumid:

1. Toimimine, mis viitab saadavate andmete täpsusele ja vajalikke ressursside olemasolule soovitud täpsuse saavutamiseks ning erinevad keskkonna tingimused, mis samuti avaldavad mõju soovitud täpsusele.

2. Vastuvõetavus, mis näitab, millisel määral on inimesed valmis vastu võtma biomeetrilist süsteemi.

3. Möödahiilimine, mis näitab, kui lihtne on petturlike tehnikate abil süsteemi petta ning keskenduda sellise riski minimeerimisele.

Uurides hilisemaid uuringuid selgub, et teoreetilised ja praktilised eeldused ja nõuded biomeetrilise tuvastamisprotsessi läbiviimiseks on samad. Muutunud on vaid lähenemine, mis tuleneb tehnoloogilisest progressist, mis annab pidevalt uusi võimalusi biomeetrilise autentimise arendamiseks. (Jain *et al* 2004:4-5)

Siinkohal leiab kinnitust varasemalt välja toodud Wayman´i seisukoht, et antud valdkonnas on põhitõed ajas muutumatud. Toetudes faktile, et igal biomeetrilise autentimise edasiarendamise ettevõtmisel lähtutakse kindlatest teoreetilistest ja praktilistest nõuetest, mis peavad omavahelises seoses alati kehtima, saab väita, et need kriteeriumid on selle valdkonna aluseks.

Biomeetrias on mitu võimalikku mõõtmisobjekti ehk biomeetrilisi andmeid saab lugeda mitmet erinevat moodi erinevatelt biomeetriliste parameetrite kandjatelt. Küsimus seisneb selles, millised olemasolevatest võimalustest on sobilikud selleks, et võtta need kasutusele maksete tegemiseks. Igal biomeetrilisel objektil on omad eelised ja puudused (vt lisa 1).

Biomeetriliste mõõtmisobjektide klassifikatsioon on laiapõhine, kuid antud töö keskendub võimalustele, mis on autori arvates sobilikumad kasutuselevõtuks maksete valdkonnas. Sellekohaselt vajavad käsitlust sellised biomeetrilised objektid, mis on seotud käe-, näo- ja okulaarse piirkonnaga. Muud biomeetrilised lähenemised on raskesti teostatavad ning mõni tunnus ei ole piisavalt unikaalne või ei ole sobilik tuvastusprotssesi teisendamise protseduuri läbiviimiseks. Näiteks nn „pehme" biomeetriline mõõtmisobjekt on seotud inimese soo, etnilise kuuluvuse, pikkuse ja armidega. Keemiline lähenemine tähendab DNA, südamerütmi ja lõhna uurimist. Käitumuslik lähenemine eeldab klahvivajutuse, allkirja, kõnnaku ja hääle käsitlemist. Toetudes sellele, saab järeldada, et kõik meetodid, mis jäävad edaspidisest käsitlusest välja, on aeganõudvad, osad on ebatäpsed ja radikaalses vaates on mõned ka absurdsed, kui võtta arvesse, et valitud meetodit peaks kasutama igapäevaselt maksevahendina. (Abbasi *et al* 2014:2673-2688)

Allpool olevas tabelis 1 tuginedes eelpool mainitud argumentidele, on välja toodud objektid, mille hulgast on autori arvates võimalik välja valida mõistlikud tunnused, mis vastaksid sellistele kriteeriumitele nagu andmete kogumise ja transleerimise lihtsus, lõppkasutaja mugavus ning turvalisus (vt. Tabel 1).

Tabel 1. Makse teostamiseks sobilikumad biomeetrilised objektid piirkonniti

Biomeetria		
Käe piirkond	Näo piirkond	Okulaarne piirkond
• Sõrmejälg • Peopesa jälg • Labakäe geomeetria • Käe veeni muster • Sõrmenukk	• Näojooned • Näo termograafia • Kõrva kuju • Keele muster	• Võrkkest • Vikerkest ehk iiris • Skleera ehk silmavalge

Allikas: Autori koostatud, (Abbassi *et al* 2014:2673-2688) põhjal

Sõrmejälg, nägu ja silmaiiris on kõige populaarsemad tunnusjooned biomeetrilise autentimise süsteemides. Nende objektidega on lihtsam organiseerida andmete kogumise ja töötlemisega seotud protseduure. (Jain *et al* 2016:80-105)

Silmaiirise struktuur kujuneb inimesel välja teiseks eluaastaks ja selle keeruline tekstuur sisaldab palju eristuselemente, mida ei saa isegi kirurgiliselt mõjutada ega võltsida selliselt, et autentimise protseduur saaks toimida. Tänu oma unikaalsuse, püsivuse ja turvalisuse omadustele on tegemist suurima potentsiaali omava biomeetrilise objektiga. Sõrmejäljed omavad unikaalsuse seisukohalt sarnaseid eeliseid, kuid võivad olla rohkem mõjutatud mõne välisteguri poolt ning kopeerimisoht on suurem. Need puudused on veelgi suuremad näojoonte meetodil, kuid teisest küljest, korrektsetes tingimustes ja keskkonnas on tegemist mugava lähenemisega autentimisprotseduurile. (Jain *et al* 2004:9-10)

Maksete kontekstis ei tekita autentimisviisi valik, mis koosneks eelpool nimetatud populaarsematest objektidest potentsiaalsetele kasutajale ebamugavusi ning ei tekita tuvastamisprotsessis liigset ajakulu.

Sõrmejälje kasutamine tundub oma omaduste poolest hea lahendusena ning on kõige populaarsem lahendus biomeetrias, kuid tegelikult välja toodud loetelu hulgast on tegemist autentimisviisiga, mille kopeerimine on piisavalt lihtne, kui käsitleda reaalajas tehinguid. Sõrmejälje kopeerimiseks on mitmeid viise, on kõrgtehnoloogilisi ja on primitiivsemaid, kuna iga inimene jätab oma sõrmejälgi peaaegu igale objektile, mida puutub (Adamek *et al* 2015: 169–176). Kui kurjategijal on olemas jäljend, siis saab ta seda kasutada ka reaalajas. Mainimata ei saa jätta ka asjaolu, et pärast biomeetrilise skänneri kasutamist, vajab üldjuhul seade puhastamist, mis on vajalik nii steriilsetel kaalutlustel, kui ka turvalisuse tagamise eesmärkidel.

Sõrmejälje kasutusega kaasnevad turvariskid on maandatavad erineval viisil. Üheks võimalikuks lahenduseks on vastavalt valitud biomeetrilise autentimise süsteemi valikule, näiteks multiobjektilisuse kasutamine või luua turvalisemad kriteeriumid ja keskkond andmete lugemise faasis, mis elimineeriksid kopeeritud jäljendi kasutuse õnnestumise tõenäosuse.

Võttes kokku erinevaid biomeetrilise autentimisega seotud mõõtmisobjekte, saab väita, et biomeetria on üldises mõistes tehniline termin, mis on seotud keha mõõtmiste kalkulatsioonidega ning on seoses inimese omadustega, mida saab käsitleda kui mõõdikuid.

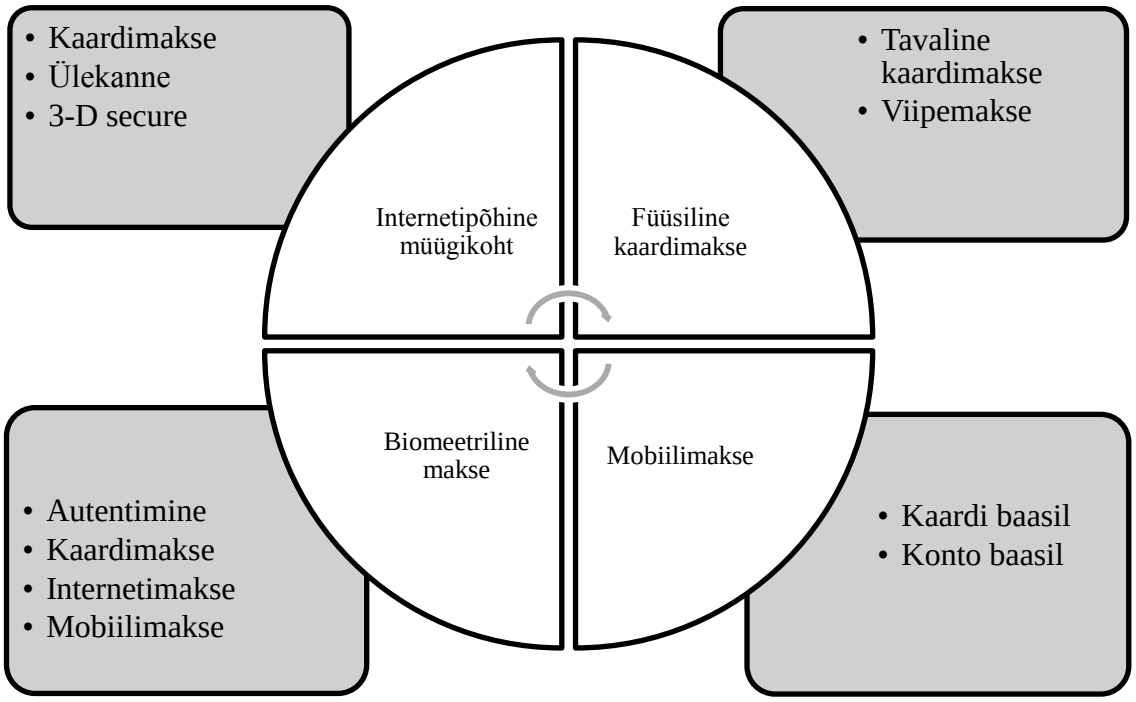
Toetudes teostatud teoreetilisele käsitlusele on käesoleva töö autor valinud välja maksete sooritamiseks sobilikumad biomeetrilisi parameetreid kandvad objektid. Nendeks on silmaiiris, sõrmejälg ja näojooned.

Oluline on teadmine, kuidas opereeritakse biomeetriliste parameetritega valitud objektidel ehk millisel kujul liiguvad andmed alustades süsteemi sisenemisest kuni andmebaasini. Toetudes erinevate autorite käsitlustele, kõigi kolme valitud variandi puhul opereeritakse piltidega ja erinevus seisneb vaid kasutatavast algoritmist. Peale andmete lugemist, tekib kujutis, millele kantakse teatud algoritmi kasutades kontrollpunktid, toiming jätkub pikslite tasandil. Seejärel konverteeritakse saadud kujutis binaarsele kujule ja saadetakse andmebaasi. Järgmises alapeatükis on käsitletud müügikohtades kasutusel olevate maksemetodite toimisloogikat biomeetriliste meetodite integratsiooni perspektiivist.

1.2 BIOMEETRILISTE MAKSETE INTEGRATSIOON KAARDIMAKSEPÕHISTE MAKSEMEETODITEGA

Selleks, et selgitada loogikat, kuidas saaks toimuda üks või teine biomeetrilise autentimise süsteem, peab käsitlema ülevaatlikult tänapäeval kasutusel olevate maksemeetoditega seotud definitsioone. Eelkõige huvitab autorit füüsilistes ja Internetipõhistes müügikohtades tehingute sooritamise võimalused ja seetõttu käsitleb autor POS (*Point of Sale*) tehingutega seotud definitsioone. Müügikohtades saab arveldada ka sularahas, kuid antud töö raames see võimalus jäetakse välja. Biomeetriline autentimine on kaardimakse autoriseerimissõnumite osa, mis on üks võimalustest tuvastusprotseduuri läbi viimiseks ja tehingu kinnitamiseks. See tähendab seda, et maksete vahendamise süsteem, alates teatud etapist ei saa erineda võrreldatuna teiste autentimismeetoditega kuna tehingu päringu liikumine peab olema kooskõlas autoriseerimisvõrkude ja teiste asjaosaliste organisatsioonide normidega. Rõhutaks, et kuna käsitletav spetsiifiline valdkond on rangelt reglementeeritud ning maksemeetodid peavad vastama standarditele, seadusandlusele ja muudele normidele, saaks oletada, et mõistete defineerimisel erinevatel autoritel lahkarvamusi ei tohiks olla. Lähtuvalt sellest, käesoleva töö autor käsitleb teemaga seotud mõisteid andes üldist ülevaadet

müügikohtades kasutuselolevatest maksemeetoditest ja nende toimimisest. Järgneval joonisel on kujutatud maksemeetoditega seonduvate mõistete skeem ja lähenemisloogika edaspidisele käsitlusele (vt joonis 3).



Joonis 3. Mõisteskeem ja lähenemisloogika uurimisprobleemile (autori koostatud).

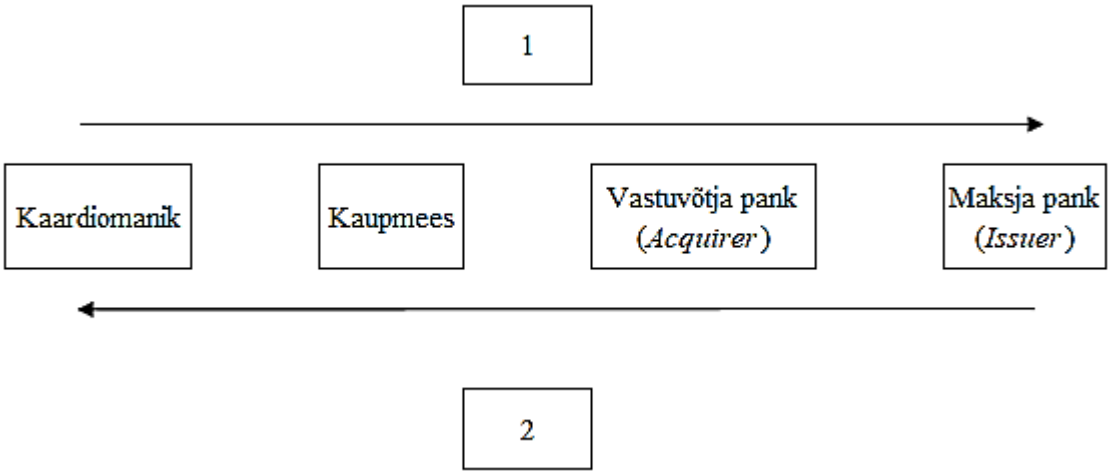
Kui vaadata joonist 3 täpsemalt, siis võib märgata huvitavat olukorda. Biomeetriline makse on välja toodud kui eraldi makse vorm, mitte lihtalt kui autentimise võimalus. Nimelt biomeetriline makse omaette oleks teoreetiliselt võimeline asendama teisi maksemeetodeid, kui seda käsitleda biomeetrilise identifitseerimise süsteemi seisukohast. Verifitseerimissüsteemi loogikast lähtudes on biomeetria vaid võimalikuks autentimismeetodiks iga maksetüübile.

Antud teemas käsitleb autor kaardimakseid, mis kirjeldavad kõige paremini kogu maksetehingute protsessi. Kaardimakse on tehingu protsess, milles kaks osapoolt teatud mõttes ei tunne teineteist ning tehingu toimumine on võimalik tänu maksesüsteemi autoriseerimisvõrgustiku olemasolule (Ward 2006:89-92). Selle definitsiooni raames on peetud silmas, et enne tehingut pole teada, mis pankade kliendid on tehingu osapooled

ning kõik saab toimuda kui on olemas ühine võrgustik, mis tegeleb autoriseerimisprotsessiga, milleks on näiteks tuntumad Visa ja Mastercard.

Eelmises alapeatükkis olid käsitletud biomeetrilise tuvastamisega seotud süsteemid. Verifitseerimissüsteemi puhul oleks käesoleva teema kontekstis tegemist tavamakse kinnitusega, kus selle teostamiseks kasutatakse autentimiseks biomeetrilisi andmeid. See tähendab seda, et selle lähenemise raames kehtivad samasugused reeglid ja käsitlused nagu kaardimaksetes.

Kaardimakse avatud keskkonnas saab toimuda vaid autoriseerimisvõrgu olemasolu korral. Üldistatud kujul võrgu toimimise loogikat saab kirjeldada järgneva joonisega (vt joonis 4).



Joonis 4. Kaardimakse valideerimise protsess (autori koostatud, Arévalo *et al* 2017:2 põhjal).

Joonisel 4 on kujutatud autoriseerimisvõrgu üldine toimimisloogika. Kaardiomanik sooritab ostu. See võib olla tavaline või Internetis olev müügikoht. Kaupmees käitleb kaardi ja tehingu andmeid ja esitab autoriseerimispäringu oma panka (*acquirer*). Makse vastuvõtja pank omakorda esitab autoriseerimispäringu kaardi väljaandnud panka (*issuer*). Kaardi väljaandnud pank kas kiidab tehingu heaks või keeldub sellest ning saadab oma autoriseerimispäringu vastuse tagasi läbides samad etapid, aga vastupidises suunas.

Kui vaadata eelpool kujutatud joonist biomeetrilise verifitseerimise süsteemi seisukohast, siis teoreetiliselt saab seda rakendada kaardiomaniku, kaupmehe ja ka maksja panga faasis. Kõik oleneb sellest, mis etappis toimub autentimine ja kus arhitektuuriliselt asub biomeetriliste mallide andmebaas.

Biomeetrilise identifitseerimise süsteemi seisukohast ei oleks tavalise kaardimakse loogika eriti sobilik ning sobib pigem kasutamiseks suletud süsteemis ehk piiratud keskkonnas.

Internetipõhiste müügikohtade kontekstis käsitletakse selliseid termineid nagu e-kaubandus või e-kommerts (*e-commerce*). E-kaubandust saab käsitleda kui globaalset turgu, milles tehingu osapooled saavad korraldada kaubandustegevust vaatamata geograafilistele piirangutele (Ahuja, Kazanchi 2016:609). E-kaubandust saab vaadelda kui äritehingut, mis säästab aega ja lahendab geograafilise piirangu probleemi, mis viib tehingu osapooled digitaalsel turul kokku ning mille teostamiseks on vajalik pangakaart (Aguilar *et al* 2015:277).

E-kaubanduses edastatakse tehing virtuaalses keskkonnas, mille teostamiseks peab klient enda autentimiseks edastama rohkem personaalset informatsiooni võrreldes maksega füüsilises müügikohas (Ashrafi, Ng 2009:321). Gurvirender ja Zareef (2017:255) on leidnud, et indiviid on haavatav sisestades oma personaalseid andmeid veebilehel e-kommertsi tehingu sooritamiseks, kuna võib langeda müügikoha ettevõtte võimaliku oportunistlikku käitumise ohvriks, mis omakorda tekitab klientides teatud määral skeptilisust e-kaubanduse suhtes, mis pidurdab valdkonna arenguprogressi.

Tõepoolest, kuna kaarti, millega soovitakse sooritada tehing Internetikeskkonnas ei ole füüsiliselt kohal, on loogiline, et nõutakse rohkem kliendi andmeid autentimise eesmärgil. Sisuliselt suurendab klient oma turvariski sisestades veebikeskkonda oma personaalset informatsiooni. See on põhjuseks, miks tänapäeval pangad ja kaupmehed on hakanud kasutama 3-D secure tehnoloogiat.

3-D secure on kõrge turvalisuse autentimise protsessi etapp, milles suunatakse kaardiomanik oma panga keskkonda tuvastusprotseduuri läbimiseks. See on loodud kaardiomaniku, kaupmehe ja panga turvalisuse tagamiseks (Mastercard…2016). Eesti

näitel on tegemist oma kaardi liitumisega turvaliste ostude nimekirjaga ning positiivne aspekt on see, et kuna vahendajaks on kliendi pank, siis ka personaalsed andmed ei ole liigselt Internetis levitatud.

Võttes kokku e-kaubandust puudutavaid definitsioone saab kokkuvõtvalt öelda, et tegemist on terminiga, mis iseloomustab kaubandustegevust Internetis, millel puuduvad distantsilised ja ajalised barjäärid ning mille sooritamiseks on vajalik pangakaardi olemasolu. Toetudes turvariski käsitlusele, kus võimalikuks ohuks tuuakse välja e-kaubanduse progressi pidurdust, on selge, et usaldusväärne ja efektiivne tuvastusprotseduur on selle valdkonna jaoks oluliseks aluseks, mis on alati aktuualne.

Siinkohal oleks riskide maandamiseks võimalikuks alternatiiviks biomeetrilise autentimise rakendamine, mis omakorda peaks olema lahendatud selliselt, et välja toodud autentimise liik ei tekitaks veelgi suuremaid riske.

Biomeetriliselt saab läheneda ka mobiilimaksetele (*m-commerce*). Hetkel on teada, et on olemas nn viipemakse funktsionaalsusega pangakaardid ja samal loogikal põhinevad ka osad mobiilimaksed.

Mobiilimakse on makse, mida saab teostada nutitelefoniga, milles on vastava panga või organisatsiooni poolt väljastatud tarkvara, asetades sarnaselt viipemakse funktsionaalsusega kaardiga oma maksevahend makseterminali kõrvale (Cocosila, Trabelsi 2016:7).

Lara-Rubio ja Liébana-Cabanillas (2017:33) on oma teadustöös võtnud arvesse erinevaid teoreetilisi käsitlusi ja andnud nende baasil mobiilimaksetele definitsiooni, mille kohaselt on tegemist tegevusega eraisiku ja/või ettevõtte osalusel, milles osaleb seade, mis on ühendatud mobiilsesse võrku, mille abil saab sooritada finantstehingu.

Alljärgnevas loetelus on selgemalt ja kokkuvõtvalt välja toodud mobiilimakse definitsioonid, kus on käsitletud erinevad mobiilimaksete tüübid (Khalid *et al* 2017:398):

1. Mobiilimakse ehk kaugmobiilimakse tähendab tehingut, mida sooritatakse mobiiliseadmega ilma otsese füüsilise kontaktita müügikohas asuvas makseterminalis,

üle mobiilse Interneti, mille raames toimub rahaliste vahendite ülekanne spetsiaalse tarkvara või SMS´i abil.

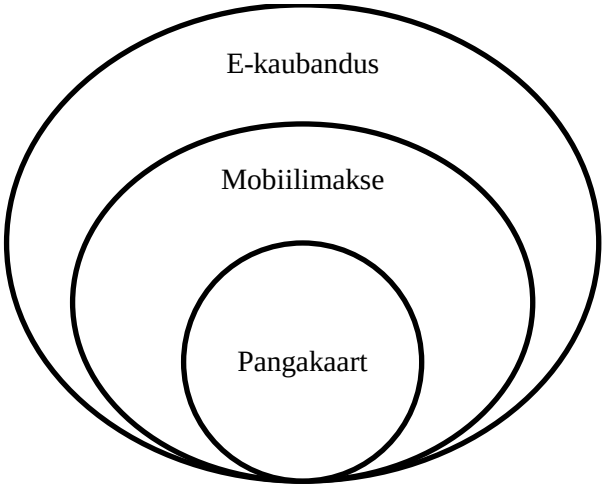
2. Kontaktivaba mobiilimakse on makse, kus indiviid maksab toodete või teenuste eest müügikohas, kasutades selleks oma mobiiliseadet ja see protsess on võimalik tänu mõlema seadme vajaliku tarkvaralise liidestuse olemasolule, kusjuures makset on võimalik ka sooritada järelevalveta müügikohas.

3. Mobiilimakse on NFC (*Near Field Communication*) tehnoloogial põhinev makse, mis on tuntud kui mobiili viipemakse, mida sooritatakse müügikohas. Seade NFC-toega koos paigaldatud makserakendusega on isikupärastatud omades seost konkreetse pangakaardi või -kontoga.

Võrreldes erinevate autorite mobiilimaksetega seotud definitsioone, saab väita, et lahkarvamusi mobiilimaksete olemuse osas ei ole. Erisused on vaid selles, et valitud definitsioonide hulgas on kokku võetud erinevate valdkondade käsitlused, mis lõppkokkuvõttes taanduvad ühisele arusaamale mobiilimakse olemuse osas. Antud töö temaatika raames on mõistlik pöörata tähelepanu mobiilimaksele, mis sisaldab isikupärastamise elementi pangakaardi sidumise näol. Sellel juhul, toetub see maksemeetod kaardimakse loogikale.

Tänapäeval võivad müügikohad ja ka nendega seotud makseviisid olla hübriidkujul. Näiteks on muutunud tavapäraseks praktikaks, kus e-kaubandus ja mobiilimakse on omavahel seoses ja on omavahel põimunud . (Hess *et al* 2016:26-37)

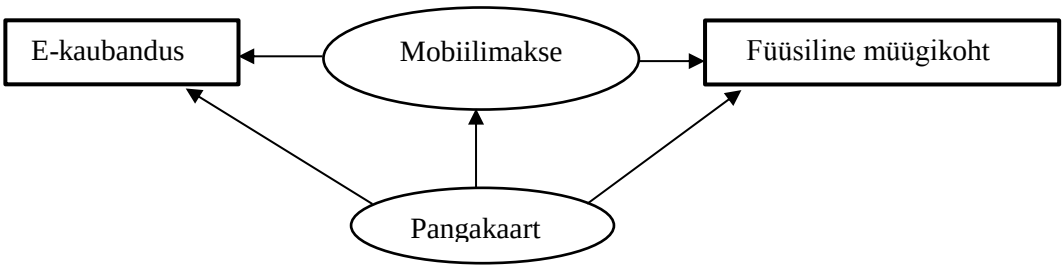
Konkurents e-kaubanduse ja maksete turul annab tõuke tehnoloogilisele arengule, mille tulemusena sünnivad uued mugavamad makselahendused müügikohtades. Kuna e-kaubanduses maksetehingu teostamiseks on vajalik pangakaart ja ka mobiilimakse aluseks on seos pangakaardiga, siis selle tulemusena ongi võimalik selline hübriidlahendus (vt joonis 5).



Joonis 5. E-kaubanduse integratsioon mobiilimaksega (autori koostatud).

Joonisel 5 on kujutatud üks võimalikest lahendustest, kuidas on ülesehitatud maksevahendite omavahelised seosed, mille lõppväljundiks on e-kaubanduses tehingu sooritamine. Siinkohal on oluline märkida, et antud käsitluses on tegemist mobiilimakse tüübiga, mida saab kasutada virtuaalses keskkonnas ning mille toimumise eelduseks on lihtsalt mobiiliseadme olemasolu ehk ei kasutata NFC tehnoloogiat ning millele üleüldiselt ei kohaldata füüsilise müügikoha makseterminaliga suhtlemisprotokolli nõudeid. Kuna mõlemad makseviisid eraldiseisvalt saavad olla realiseeritud pangakaardi olemasolu korral, siis ka hübriidlahenduses on see aluseks.

Toetudes erinevate eelpool välja toodud müügikohtade tüüpidele ja nende käsitlustele ning võttes arvesse, et iga tehingu sooritamiseks on vajalik autoriseerimisvõrk, mille kasutuse eelduseks on pangakaardi olemasolu, siis saab väita, et kõige aluseks on pangakaart ning makseviisid võivad omavahel põimuda (vt joonis 6).



Joonis 6. Kaardi baasil makseviiside võimalused müügikohtades (autori koostatud).

Eespool välja toodud jooniselt on näha, et erinevat tüüpi müügikohtades saab tasuda otse pangakaardiga või saab seda teha mobiiliseadme vahendusel, kuid muutumatuks jääb protsessi eeldused, milleks on pangakaardi kasutus.

Biomeetrilise verifitseerimise süsteemi kohaselt, kus biomeetrilisi parameetreid kasutatakse salasõna, PIN´i või mõne tuvastusseadme asendamiseks, on võimalik tugineda tavalisele kaardimakse loogikale. Muutusi üldises makse protsessis sellise süsteemi rakendamiseks ei ole. Oluline on vaid ära määratleda, mis faasis ja kelle või mille poolt teostatakse biomeetrilist tuvastusprotseduuri.

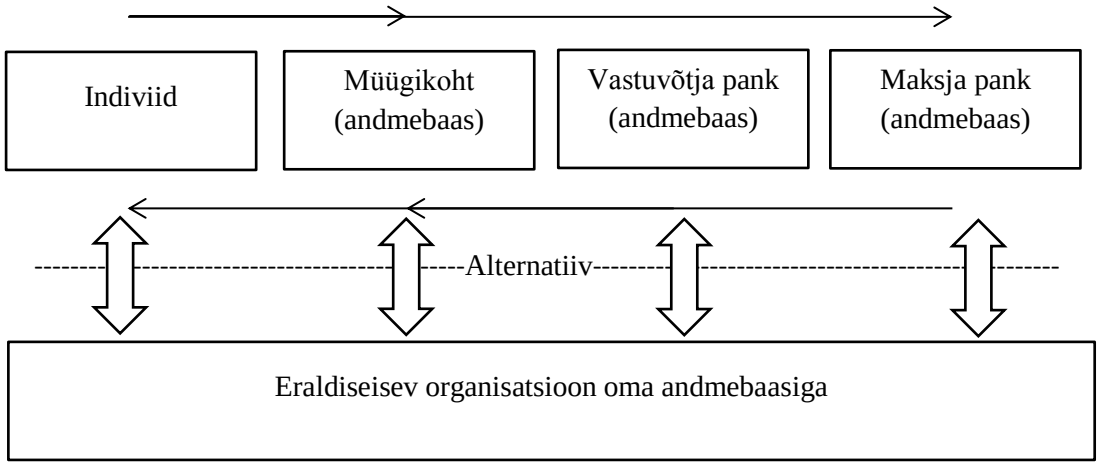
Kuna kaardimakse autoriseerimispäringu liikumise loogika biomeetrilise verifitseerimise rakendamisel ei muutu, siis ei tähenda selle rakendamine pankade ja autoriseerimisvõrkude jaoks võimalikku tulu kahanemist nii makse sooritaja kui ka makse vastuvõtja panga seisukohast. Pigem tõuseb makseprotsessi juures selle turvalisus, mis on nii autoriseerimisvõrgu ja pankade, kui ka klientide huvides. Klientide all on mõeldud kaupmehi ja müügikohas oste sooritavaid isikuid.

Biomeetrilise identifitseerimise süsteemi rakendamise korral oleks maksete valdkonnas toimumas ulatuslikud muutused. Loomulikult on võimalik siduda mõni biomeetriline parameeter sobiliku lisavahendiga ka identifitseerimise süsteemis. Üldisemas mõttes on biomeetria kontekstis tegemist unikaalse autentimise instrumendiga, mis kokkuvõttes on ühelt poolt unikaalne, kuid teiselt poolt on tegemist siiski staatilist omadust omava väärtusega. Algoritmid ja andmete konverteerimise meetodid võivad olla erinevad, kuid biomeetriliste andmete algallikas on muutumatu, kui vaadelda maksete sooritamiseks enam sobilikumaid biomeetrilisi mõõtmisobjekte.

Teoreetiliselt saab biomeetrilise identifitseerimise süsteemi rakendada toetudes verifitseerimise süsteemi toimimisloogikale, mis omakorda tugineb autoriseerimisvõrgu loogikale. Sellisel juhul tuleb arvestada biomeetrilise autentimise süsteemide erisustega ning arvesse võtma potentsiaalset suuremat turvariski, kuna biomeetrilise identifitseerimise süsteemi korral on indiviidi biomeetriline andmekandja samal ajal nii kasutajatunnus kui ka parool.

Oluliseks küsimuseks kujuneb, millises tehinguahela faasis peaks olema salvestatud mallide andmebaas ja mis rolli andmete edastuses mängib iga ahelas olev osaleja. Hetk, millest alates algab identifitseerimisprotseduur, kas kliendi või müügikoha poolt, oleneb sellest, kas klient alustab makset otse makseterminalis või näiteks kasutades selleks isiklikku seadet, kus edaspidi toimiks makse protseduur vastava mobiilimakse käsitluse loogikale.

Kuna biomeetrilise identifitseerimise süsteemis oleks tegemist sensitiivsete isikuandmete haldamisega, siis oleks võimalik tehingute liikumise struktuuri lisada väline faktor, milleks oleks eraldiseisev organisatsioon, mis vähendaks isikuandmete lekete võimalikke kohtade arvu ning kogu süsteem oleks usaldusväärsem. (vt. Joonis 7).



Joonis 7. Makse liikumise võimalused identifitseerimise süsteemis, autori koostatud tuginedes (Arévalo *et al* 2017) ja (Lumini, Nanni 2017) käsitlusele.

Üleval oleval joonisel 7 on üldistatud kujul kujutatud autori nägemus kahest võimalusest, kuidas saaks rakendada biomeetrilise identifitseerimise süsteemi maksete kontekstis. Ühe võimaluse aluseks on verifitseerimissüsteemi kaardimakse loogika. Alternatiivina on välja pakutud eraldiseisev organisatsioon, mis tegeleb salvestatud mallide haldamisega ning läbi selle, teostab ise vajalikke toiminguid erinevate ahelas olevate faaside osapooltega.

Esimese võimaluse puhul saab lokaalsel tasandil hoida oma malle müügikoha andmebaasis ja vastavalt valitud edaspidisele arveldusmeetodile võiks see olla ka kogu süsteemi lõpp-punktiks. Teisest küljest, koheste finantsvahendite saamiseks peab

protsess läbima kõik ahelas olevad punktid ja minema kuni maksja pangani ja tagasi. Sellise lahenduse puhul mängib makse vastuvõtja pank vaid edastaja rolli ja salvestatud malle haldama ei ole kohustatud.

Biomeetrilise identifitseerimise süsteemi kasutamine maksete sooritamiseks, arvestades asjaolu, et tegemist on personaalsete ja ajas muutmatu andmetega püstitab küsimuse, kas on üldse võimalik selle organiseerimine ilma mõne muu biomeetrilise objekti või abivahendi kasutuselevõtmiseta.

Arvestades biomeetrilise autentimise ja müügikohtades kasutusel olevate maksemeetodite käsitlusi ning tuginedes nende sisule ja toimimisloogikale, saab kokkuvõtlikult öelda, et biomeetriline makse on maksetehingu sooritamise viis, mille teostamiseks kasutatakse biomeetrilisi meetodeid. Järgmises peatükis on käsitletud biomeetriliste maksetega seotud praktilisi lähenemisi, mis tuginevad teoreetilistele seisukohtadele ja kirjeldavad käesoleva töö autori uurimismetoodikat, mis oli kasutatud uuringu läbiviimiseks ning ka uuringu tulemused.

2. BIOMEETRILISTE MEETODITE RAKENDAMINE OLEMASOLEVATESSE MAKSEMEETODITESSE

2.1 UURIMISMETOODIKA JA VALIM

Käesolevas peatükis teeb autor ülevaate varasemalt teostatud teaduslikest empiirilistest uuringutest; asjaosaliste organisatsioonide turu-uuringutest ja seisukohtadest; kirjeldab olemasolevaid lahendusi ja tehnilisi aspekte, millega peab arvestama biomeetria kasutuselevõtmise korral. Selline lähenemine on käesoleva töö uurimismetoodika aluseks, mille tulemusena on võimalik saavutada adekvaatseid autoripoolse uuringu tulemusi. Selleks, et saavutada töös püstitatud eesmärki, peab olema mitmekülgne ülevaade, mis tugineb ka varasematele uuringutele. Valitud uurimismeetod aitab luua poolstruktureeritud küsimustiku selliselt, et uuringu tulemusel oleks võimalik asjakohane praktiline väljund.

Biomeetrilise identifitseerimise ja verifitseerimise puhul võib potentsiaalsel kasutajal tekkida sellised küsimused nagu:

- Kas biomeetriline süsteem suudab õigesti inimest tuvastada?
- Kui suur on oht, et andmed kopeeritakse kuritegevuslikel eesmärkidel.

Nendele küsimustele aitavad vastata varasemad empriilised uuringud, mis käsitlevad tuvastusprotseduuri täpsusi erinevatel ajavahemikel. Need uuringud on tehtud suurte andmemahtudega, mis pärinevad USA valitsuse biomeetriliste andmete andmebaasist ning mis toimusid valitsuse järelevalve all. Valitud uuringud on välja toodud kirjeldamaks tuvastuprotseduuri täpsuse tendentsi ajas.

Phillips *et al* (2007:1-55) näo ja silmaiirise tuvastuse algoritmide uuringus on välja toodud vigade protsendid teatud ajaperioodi jooksul. Aastal 1993 oli näo tuvastuses valetuvastusemäär 79%. Aastal 2006 oli see näitaja juba 0,1%, kuid olenevalt kasutatud metoodikast esines 1-2,5% katsetes olukordi, millal süsteem ei suutnud üldse isikut tuvastada. Silmaiirise puhul oli 2006 aasta seisuga valetuvastusmäär 0,1% ja olukordi, kui süsteem ei suutnud tuvastada olenevalt valitud metoodikast 1,1-1,4%. Uuringu läbiviimisel toimetati 38 001 subjektiga, millelt oli loodud 205 602 kujutist.

Sõrmejäljetehnoloogias olid head tulemused saavutatud juba aastal 2003, kui valetuvastusemäär oli 0,01% ja ei suudeta tuvastada 0,6% olukordades ning seejuures oli kasutatud 12 000 erinevat sõrmejälje kujutist. (Wilson *et al* 2004)

Kolm enam sobilikumat maksete valdkonna kontekstis biomeetrilist objekti kinnitavad ka Anil K. Jain´i (2016:80-105) seisukohta. Näiteks sellise objekti kasutusele võtt nagu hääl, ei ole otstarbekas maksete kontekstis kuna täpse tulemuse saamiseks peavad keskkonna tingimused olema ideaalsed ning tegemist on biomeetrilise objektiga, mis ajas muutub. (Martin, Przybocki 2004:12-22)

Eespool välja toodud empiirilised uuringud kinnitavad varasemalt käsitletud teoreetilist seisukohta, et tehnoloogiline areng on põhiline faktor, mis viib antud valdkonda edasi. Lisaks tehnoloogilisele arengule on oluline ka kasutatav algoritm. Teisisõnu, ka tänapäeval võib saavutada nii täpseid kui ka ebatäpseid tulemusi kuna kõik sõltub valitud vahendite kasutamisest. Maksete valdkonnas on täpsus primaarseks tingimuseks, et lahendus saaks korrapäraselt toimida.

Vastates teisele potentsiaalselt võimalikule küsimusele turvalisuse kohta, siis siinkohal pole kindlat garantiid olemas. Risk on suur, kui rääkida maksetest identifiseerimise süsteemis. Teisest küljest lähtuda tuleks põhimõttest, et andmete lugemise ja töötlemise meetod ja asukoht peab olema võimalikult korrektne, mis tähendab, et kogu väljaehitatav süsteem peab olema detailideni läbimõeldud.

Edaspidi on välja toodud kaks pilootprojekti, mis on korraldud asjaosaliste organisatsioonide poolt, kellel on sarnaste uuringute jaoks vajalikke vahendeid.

Prantsusmaa pangad on 2012. aasta pilootprojekti raames katsetanud biomeetrilist autentimist pangasiseste maksete sooritamiseks. Projektis said osaleda ka müügikohad. Testimisperioodi ajaks olid tekitatud vajalikud abivahendid (kaart või mobiilirakendused), mis näitab, et biomeetriliste meetodite vastu on huvi ka pankadel. (French Banks…2012:2)

Põhjalikuma analüüsiga on aga Mastercard´i (90% of Dutch…2016:2) pilootprojekt, mis leidis aset 2016. aastal, milles rakendati näo- ja sõrmejäljetuvastust Internetimaksetel. Projekt viidi läbi Hollandis ja tegemist on ristkasutusega ehk tehinguid sai teostada iga kaupmehe juures, kellel oli olemas vastav leping Mastercard´i aktsepteerimiseks ning mis toimus sõltumata pangast, kellega oli kaupmehel sõlmitud leping. Pilootprojekti tulemused olid positiivsed. 95% sõrmejälje ja 80% näotuvastustehnoloogiat kasutanud kliendid ütlesid, et tegemist on väga mugava lahendusega. 75% osalenutest arvasid, et biomeetrilised meetodid on palju turvalisemad kui tavalised tuvastusmeetodid.

Käesoleva töö autor on välja selgitanud, kuidas ja millest lähtudest saaks toimida makse biomeetrilise verifitseerimise süsteemis toetudes autoriseerimisvõrkude loogikale ja kehtivatele makseterminalidele kehtestatud reeglitele. Kuna valdkond on rangelt reglementeeritud, siis võimalikud tulevased empiirilised uuringud peaksid arvestama teatud protseduurilisi reegleid ja aluseid.

Autoriseerimispäringute baasreeglid on kirjeldatud Mastercard´i (Transaction Processing… 2017) ja Visa (Visa Core… 2015) spetsifikatsioonides. Need spetsifikatsioonid ei ole staatilise iseloomuga ja on muutuvad koos tehnoloogia arenguga ning institutsionaalsete ja regionaalsete regulatsioonide uuenemistega. Erinevates maailma piirkondades on kohati ka erinevad reeglid. Neid spetsifikatsioone on palju ning üldisemad dokumentatsioonid on avatud igale soovijale tutvumiseks, kuid spetsiifilisemad Mastercard´i (Customer Interface… 2010) ja Visa (Visa DMSA..2017) dokumentatsioonid on üldjuhul piiratud ligipääsuga, mis on olemas pankadel ja teistel autoriseerimisvõrgu partneritel ning need omakorda hargnevad vastavalt soovitud lahenduse käsitlusele.

Kui biomeetriline luger asub maksekaardil, siis sisuliselt suuri muutusi autoriseerimissõnumite liikumises ei tule, sest kõik on ära lahendatud kaardiomaniku kaardi kiibipõhiselt ning autoriseerimissõnumis on lihtsalt muudetud teatud ISO-8583 standardil põhinevate saadetavate autoriseerimissõnumite väljade positsioonid, mis vastutavad kaardiomaniku autentimisviisi kirjelduse eest (Nets Payment…2017). Pankade süsteemid peavad siinkohal olema valmis ka neid väärtusi aktsepteerima. Praktikas ei tähenda see seda, et iga pank peab tõlgendama biomeetriliste andmete sisu. Teades, et autentimine toimub kaardi sees, siis autoriseerimisvõrgu organisatsioonid annavad ette kas numbrilise või tähestikulise väärtuse, mis peab sisalduma saadetavas päringus. Teisest küljest, peavad ka makseterminalid omama tarkvara, mis on võimeline uusi sõnumiväärtusi vastavasse panka edastama korrektsel kujul.

Kuna biomeetriline autentimine võib toimuda maksevahendi väliselt, näiteks müügikoha terminalis, siis peab selleks vastava seadme tarkvara olema ülesehitatud vastavalt EMV (Europay, Mastercard, Visa) standarditele, millele toetuvad ka maksekaardid. Eelkõige on tegemist rahvusvahelise standardite kogumiga, mis võimaldab erinevatel kaartidel toimida rahvusvaheliselt autoriseerimisvõrkudes erinevates makseterminalides ning mille aluseks on kaardi kiibi ja PIN´i tehnoloogia. (EMVCo…2018)

Kui rakendada verifitseerimise süsteemi makseterminali põhiselt, siis see tähendab täiendavatele nõuetele vastamist. Kõik oleneb lõppkokkuvõttes sellest, kus hoitakse biomeetriliste andmete malle ja kuidas on organiseeritud nende sidumine kaardiandmetega. Kogu protsess peab olema vastavuses PCI (Payment Card Industry) nõuetega ning läbima teatud audiitorkontrolli. (PCI SSC…2018)

Lõppkokkuvõttes peab seade omama vastavaid sertifikaate, mis kinnitavad, et on läbitud tark- ja riistvaraline ning kaardiprodukti kontroll, mille tulemusena saab seadet võtta kasutusele kuna on vastavuses kindlate kriteeriumitega. (EMV in…2017)

Arvestades ülalmainitud nõudeid, saab järeldada, et seni tehtud empiiriliste uuringute hulgas on domineerivad need, mis kas keskenduvad ankeetküsitlustele või üldistele toimimismehhanismidele kuna pilootprojektide loogikal põhinevaid uuringuid, milles oleks korrektselt organiseeritud iga etapp, mis kokkuvõttes annaks usaldusväärse ja

positiivse tulemuse, on keeruline saavutada puuduliku ressurssi faktori tõttu. Eksisteerib ka eetiline moment, mille kohaselt tekkib küsimus, et kas saab toimetada minimaalsete vahenditega kellegi personaalsete andmetega riskides. See tähendab, et konkreetselt maksetega seonduvates empiirilistes uuringutes on usaldusväärsed tulemused vaid asjaosaliste organisatsioonide poolt teostatud uuringutes.

Kuna e-kaubandus viimastel aastatel näitab arengutendentsi, siis on huvitav, millised eelistused on inimestel selles valdkonnas biomeetrilise autentimise kontekstis. Kim´i ja Ogbanufe (2018:1-14) empiiriline uuring annab hea ülevaate tarbijate autentimise eelistusest ning selle uuringu aluseks on lisaks tehnilisele taustale ka indiviidide tajumis- ja otsustusvõime. Valimis oli 300 inimest. Katse tarbeks oli loodud lihtne e-kauplus, milles sai sooritada oste kolmel võimalikul viisil:

1. Krediitkaart
2. Krediitkaart+PIN, kus PIN on juhuslik kinnituskood.
3. Biomeetria (sõrmejälg), kus oli biomeetriline parameeter seotud krediitkaardiga.

Allpool olevas tabelis on välja toodud uuringus püstitatud hüpoteesid ja nende tulemused (vt tabel 2).

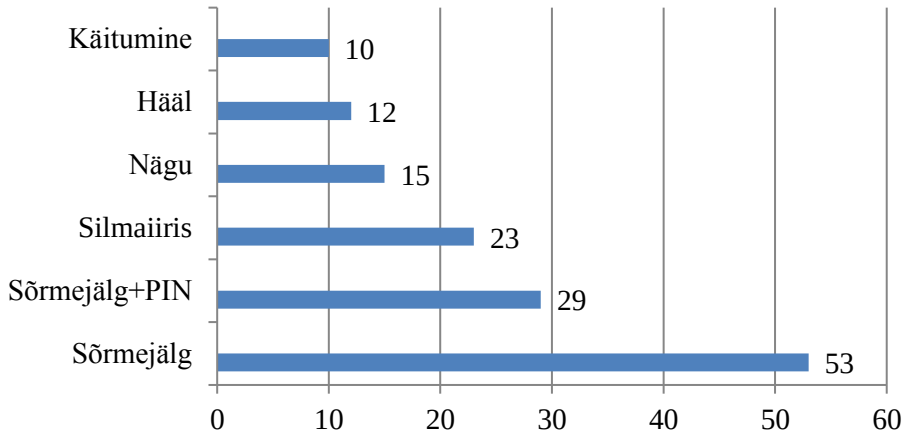
Tabel 2. Biomeetrilise autentimise võrdlus teiste makse autentimise võimalustega

Hüpoteesid		Tulemused (hüpoteesi kehtivus)	
Biomeetriline lähenemine		Krediitkaart	Krediitkaart + PIN
1	Biomeetriline autentimine on turvalisem kui teised võimalused	jah	jah
2	Biomeetriline autentimine on mugavam kui teised võimalused	ei	ei
3	Biomeetriline autentimine on sobilikum kui teised võimalused	jah	ei
4	Biomeetrilist autentimist võimaldavad müügikohad on usaldusväärsemad.	jah	ei
5	Biomeetrilst autentimist võimaldavad müügikohad tekitavad klientides lojaalsust.	ei	ei

Allikas: Autori koostatud, Kim ja Ogbanufe (2018:9) põhjal.

On oluline märkida, et kui püstitatud hüpoteesid ei leidnud kinnitust, siis tegelikult eelistus ei olnud vastupidine, vaid pigem oli tulemus sarnane.

Visa poolt (European consumers…2016:1-2) on tehtud uuring, mille eesmärgiks oli välja selgitada biomeetrilistele maksetele potentsiaalset turgu Euroopas. Selle kohaselt viidi läbi uuring seitsmes riigis, milleks olid Inglismaa, Rootsi, Hispaania, Prantsusmaa, Saksamaa, Itaalia ja Poola. Vastajaid oli 14 236 inimest ning on öeldud, et keskmiselt iga riigi kohta oli 2000 vastajat. 51% vastanutest soovisid, et kasutusel oleksid biomeetrilised maksevahendid, kellest omakorda 33% arvasid, et see on ideaalne lahendus, sest ei pea muretsema kaotatud või varastatud pangakaardi pärast. Vastajad olid arvamusel, et sõrmejäljetehnoloogia on kõige turvalisem. Alloleval joonisel on välja toodud, mis tuvastusmeetodit eelistasid vastajad (vt joonis 8).



Joonis 8. Biomeetriliste tuvastusmeetodite eelistused protsentides (%).
Allikas: Autori koostatud, (European consumers…2016:1-2) põhjal.

Kõik, kes pooldasid biomeetrilist lahendust said valida mitu võimalust, siit ka protsentuaalsed tulemused, mille summa ületab 100. Mõne autentimisviisiga on raske nõustuda kuna on raske ette kujutada, kuidas mõnda valikus olevat lahendust saaks müügikohas kasutada. Käitumise hindamist tegelikult ei saagi eriti rakendada, kui on soov teha tehinguid mugavalt, kiiresti ja turvaliselt. Osa vastanutest arvas, et pärast sõrmejälje lugemist võiks makseterminal nõuda siiski ka pin-koodi.

Eespool mainitud empiiriliste uuringute temaatika sobib ka mobiilimaksete temaatikasse biomeetrilise autentimismeetodi rakendamiseks.

NFC maksed on tänapäeval võimalikud nii android kui ka iOS platvormidel ning tuntumad on vastavalt Google Wallet ja ApplePay (Khalid et al 2017:398). Käesoleval hetkel on Google Wallet´i uus nimetus Google Pay (Google Pay…2018). Mõlema makseviisiga saab käesoleval hetkel Eestis makseid sooritada, kui makseterminal toetab NFC funktsionaalsust, kuid Eesti pankade klientidele ei ole selline makseviis kaardi välja andnud panga seisukohast võimalik. Teisisõnu, on olemas vaid makse vastuvõtmise võimalus, mis on avatud välismaalastele, kelle riikides puuduvad eespool nimetatud maksevõimaluste kasutamiseks regionaalsed piirangud.

ApplePay ja Google Pay biomeetriline autentimine on ära lahendatud mobiiliseadme siseselt. Biomeetrilist autentimist kasutatakse vaid seadmesse sisselogimiseks ja edasi toimib tavaline viipemakseloogika, millel võib olla vastavalt regulatsioonidele kehtestatud maksimaalne tehingu limiit. See tähendab seda, et viipemakse piirsumma ületamisel peab kasutama füüsilist pangakaarti ja sisestama PIN-koodi. Eestis on aga üks teenusepakkuja, milleks on Pocopay, mille mobiilirakenduses saab kinnitada tehinguid biomeetriliselt, kuid vaid ülekannete korral (Sõrmejäljega… 2016). Viimasel ajal on nutitelefonide panga rakendustes tehingute kinnitamiseks populaarseks muutunud Smart ID, kus peab kasutaja teadma oma loodud PIN-koode (Smart ID…2018). Seda rakendust kasutatakse ka erinevate keskkondadesse sisselogimiseks. Viimase puhul, kuna tuvastusprotseduur toimub seadmesiseselt, siis heaks alternatiiviks oleks kasutada just biomeetrilist meetodit.

Kogu maksete valdkond peaks osutama suurt tähelepanu biomeetrilistele meetoditele kuna asjaosalistel organisatsioonidel on oma mõjuvõimsate positsioonide tõttu võimalus dikteerida tingimusi, mida peab varem või hiljem arvesse võtma. Kellel toimub see üleminek kiiremini, see saavutab ka turueelise teenusepakkujate hulgast. See on midagi, millest võiks iga Eestis olev pank mõtiskleda.

Maailma kaks suurimat maksekaardi organisatsiooni Visa ja Mastercard on käivitanud globaalsed biomeetriliste maksete projektid ja liiguvad selles suunas, et see oleks dominantseks jõuks kaardimaksete turul. Kusjuures Mastercard teeb selliste kaartide aktsepteerimise pankade jaoks kohustuslikuks alates aprillist 2019. Üks põhilistest biomeetrilist autentimist toetavate kaartide tootjatest, milleks on ettevõte Gemalto, on loonud kaardi, kus sõrmejälje autentimine toimub kaardiomaniku kaardil ning

sõrmejälje kontrolli teostab maksekaardil olev kiip kuhu on salvestatud indiviidi õige biomeetriline mall. (Mastercard and Visa… 2018:1)

Juba aastast 2015 oli märgata, et Mastercard ja Visa on biomeetrilise temaatika prioritiseerinud enda jaoks ning on tehtud ühist tööd ühise spetsifikatsiooni loomise nimel. (Mastercard and Visa… 2015:11)

Mastercard´i ja Visa biomeetrilist autentimist kasutatavate kaartide kasutusele võtmise kohustus ei tähenda veel, et mõne aja pärast on selline kaart olemas igal inimesel Eestis. See puudutab esialgu vaid pankasid, kes peavad oma süsteeme täiendama, et oleks selliste kaartide aktsepteerimine võimalik. Hetkeolukorras tähendaks see, kui Eesti riiki tuleks välismaalane, kellel oleks vastav kaart olemas, saaks ta oma tehingud sooritatud.

Töö eesmärgi saavutamiseks valis käesoleva töö autor uuringu teostamiseks kvalitatiivse lähenemise. Selline lähenemine on sobiv uurimisprobleemile, mille tulemus on raskesti ennustatav.

Sarnaselt selles töös varasemalt käsitletud Visa poolt teostatud uuringu osalisele metodoloogiale, korraldas käesoleva töö autor oma uuringu, kuid arvestades Eesti spetsiifikat. Küsitluses käsitleb autor biomeetrilise verifitseerimise ja identifitseerimise süsteemi loogikal põhinevaid lahendusi; uurib tuvastusmeetodite eelistusi välja valitud võimaluste hulgast; selgitab välja kuidas peaks biomeetrilise maksemeetodi protseduur olema organiseeritud; võrdleb biomeetrilisi maksemeetodeid käesoleval hetkel kasutusel olevate maksemeetoditega ning selgitab välja tarbijate suhtumist nende meetodite omavahelisesse integratsiooni ja kasutamisse üldiselt.

Toetudes Visa valimi meetodile ning arvestades vastanute protsenti rahvaarvu suhtes, saaks oletada, et Eesti mastaabis võiks valimi suurus olla vahemikus ligikaudu 35-200. Seda ei saa kindlasti aluseks võtta, sest uuringus oli välja toodud keskmine näitaja, seega võib eeldada, et suurema rahvaarvuga riikides, oli ka suurem vastanute arv. Arvestades ülaltoodud asjaolusid, seadis käesoleva töö autor valimi eesmärgiks 100-200 inimest.

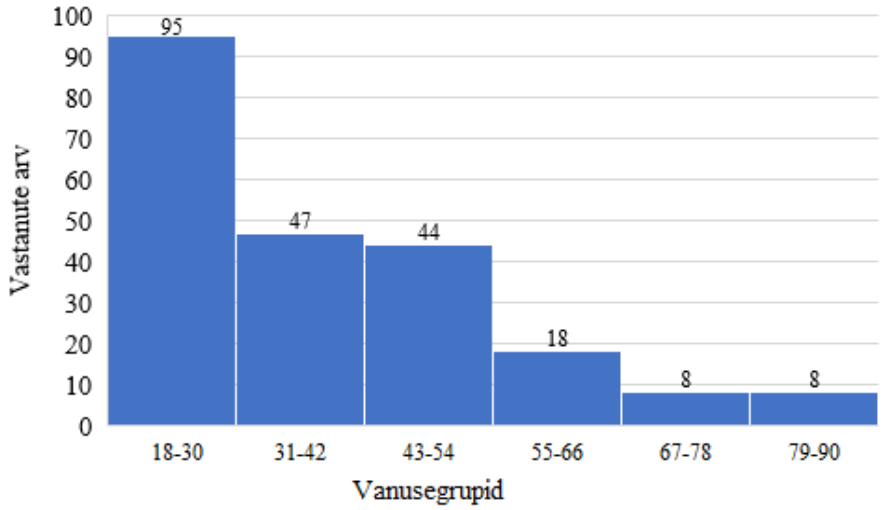
Püstitatud eesmärgi saavutamiseks oli käesoleva töö autori poolt koostatud ankeetküsitlus, mis tuginedes teoreetilisele baasile, varasemate empiiriliste uuringutele

ja makselahenduste rakendamise nõuetele, mis olid autori poolt välja selgitatud (vt lisa 2). Ankeedi üldine ülesanne oli hinnata potentsiaalsete tarbijate suhtumist maksetesse, mida saab teostada biomeetrilisi omadusi kasutades. Toetudes teoreetilise ja empiirilise käsitluse argumentidele olid biomeetrilised objektid, millelt andmeid loetakse, limiteeritud kolmele võimalusele, mis arvestades nende omadusi, oleksid enam sobilikumad maksete konteksti. Nendeks olid: sõrmejälg, silmaiiris ja nägu. Esitatud küsimused võimaldasid vaadelda uurimisküsimust nii biomeetrilise verifitseerimise kui ka identifitseerimise süsteemi seisukohast. Saadud vastused annavad ülevaate sellest, kuidas võiksid olla organiseeritud makseprotseduuri erinevad etapid või millised on tarbijate ootused antud lahenduse suhtes ning millega peab arvestama biomeetrilise lahenduse rakendamisel.

Küsimused olid edastatud paberkandjal ja e-maili teel. Selline lähenemine võimaldas küsitleda erinevas vanuses inimesi ning luua valimiga kontakti, mis suurendas tagastavate ankeetide arvu. Valimisse kuulusid Eestis elavad inimesed, kes on vähemalt 18-aastased. Kuna tegemist on uuringuga, mis puudutab biomeetrilisi makselahendusi, millega suurem osa inimestest pole varasemalt kokku puutunud, siis suurem osa vastanutest said enne ankeedi täitmist kokkuvõtlikku kirjelduse, mis oli piisav selleks, et saada küsimustest õigesti aru ning samas, mis ei olnud suunavaks faktoriks küsimustele vastamisel. Pooled vastanutest esindavad panganduse ja finantstehnoloogia sektorit ning ettevõttete esindajaid, kes tegelevad jaemüügiga. Teine pool vastanutest olid muude valdkondade esindajad, kellega sai kontakti läbi loodud kommunikatsiooni ahela, mille loomise eelduseks oli võimalikult erineva taustaga inimeste kaasamise, kes olid motiveeritud uuringus osalemiseks.

2.2 BIOMEETRILISTE MAKSEMEETODITE POTENTSIAALI HINDAVA ANKEETKÜSITLUSE TULEMUSED

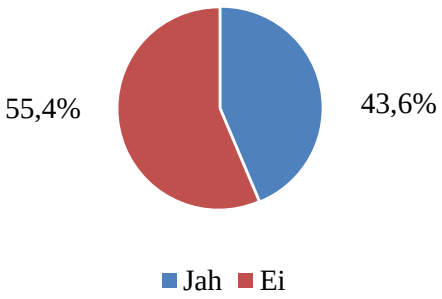
Kokku oli vastajaid 220, mis ületas käesoleva töö autori varasemalt paika pandud soovitusliku vahemikku, milleks oli 100-200. Noorim vastaja oli 18-aastane ja vanim 82-aastane. Kuna antud töö teema on suunatud tulevikule, siis prioriteet oli siiski asetatud noorematele vanusegruppidele (vt joonis 9).



Joonis 9. Vastanute jaotus vanuse alusel (autori koostatud).

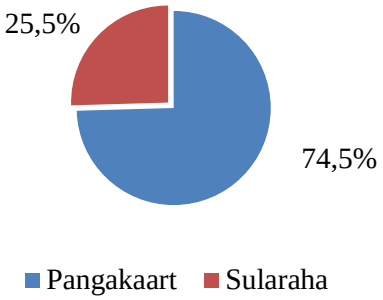
Selleks, et välja selgitada inimeste teadlikust biomeetrilistest meetoditest, oli küsitud, kas nad on varasemalt biomeetrilise autentimise temaatikaga kokku puutunud mingil kujul. See kokkupuude võis olla erineval kujul alates pealiskaudsest, kui isik on varasemalt sellest kuulnud või lugenud, lõpetades otsese kasutamisega.

Osad nutitelefonid ja sülearvutid toetavad biomeetrilist autentimist. Meedias ja filminduses käsitletakse samuti piisavalt palju biomeetrilist temaatikat. Eesti riigis isikut tõendavate dokumentide taotlemisprotseduuri korral salvestatakse andmebaasi sõrmejäljed, mis on ka kodeeritud dokumentide sisse. Arvestades ülalpool maninitud argumente olid teadlikust puudutava küsimuse vastused üllatavad, mille kohaselt on mingil määral kokkupuudet antud teematikaga ainult 43,6% vastanutest (vt joonis 10).



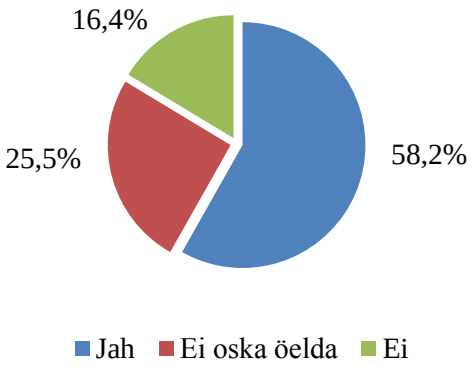
Joonis 10. Varasem kokkupuude biomeetrilise autentimise temaatikaga (autori koostatud).

Kuna biomeetriline autentimine maksete sooritamisel põhineb kaardimakse loogikal, siis järgmisena oli uuritud, mis on vastanute eelistus maksemeetodi valikul müügikohas tasumisel (vt joonis 11). Valikus oli pangakaart ja sularaha. See küsimus võimaldab tulevikus hinnata, kas need kes kasutavad sularaha, oleksid huvitatud biomeetrilistest meetoditest. 74,5% vastanutest eelistavad pangakaardi kasutamist.



Joonis 11. Maksemeetodi eelistus toodete või teenuste eest tasumisel müügikohas (autori koostatud)

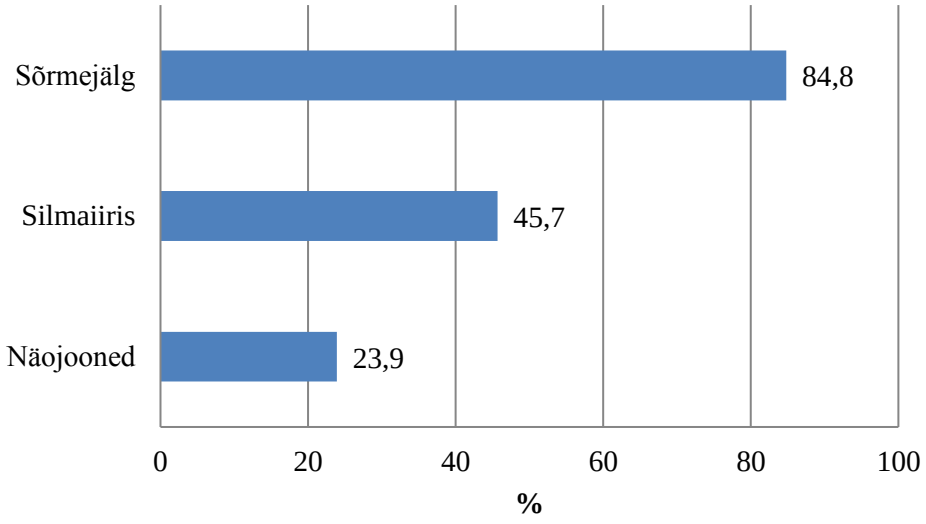
Järgmisena oli vastajatele kirjeldatud, mida tähendaks biomeetriline autentimine maksete teostamisel ning välja pakutud kolm võimalust, millelt saaks andmeid lugeda, milleks olid sõrmejälg, näojooned ja silmaiiris. Seejärel oli küsitud, et kui oleks võimalus tasuda biomeetriliselt, kas Te kasutaksite sellist võimalust (vt joonis 12). Vastusevariante oli kolm: jah, ei oska öelda ja ei. Need, kes valisid eitava vastuse, ei pidanud enam järgnevatele küsimustele vastama. Selle tulemusena jätkasid ankeedi täitmist 184 inimest.



Joonis 12. Biomeetriliste maksete potentsiaalsed kasutajad (autori koostatud).

Sularaha eelistajate vastused jagunesid põhiliselt kahte kategooriasse. Vaid üksik vastaja soovis kasutada biomeetrilist autentimist, ülejäänud vastused jagunesid enam-vähem pooleks variandi „ei“ ja „ei oska öelda“ vahel. Huvitaval kombel on negatiivse või kahtleva suhtumisega sularaha kasutajad vanemate vanusegrupide esindajad ja üldistatud kujul saab öelda, et alates varasemalt välja toodud neljandast vanusegrupist on huvi antud teema vastu minimaalne.

Need vastajad, kes oleksid huvitatud biomeetriliste meetodite kasutamisest ja need, kes ei vastamise hetkel ei osanud oma soovi hinnata, jagasid arvamust, millelt oleks nende arvates sobilikum või mugavam biomeetrilisi andmeid lugeda (vt joonis 13). Kuna potentsiaalselt saab autentimisprotseduuri teostada erinevatelt biomeetriliste andmete kandjatelt, siis antud küsimuse juures sai valida mitu võimaliku varianti kolme võimaluse hulgast. Selle tulemusena on jooniselt näha, et protsentuaalsed tulemused esindavad konkreetset valikut, mitte vastanute arvu. Suurt üllatust tulemustes ei tulnud, sest populaarsemaks valikuks osutus andmete lugemine sõrmejäljelt.

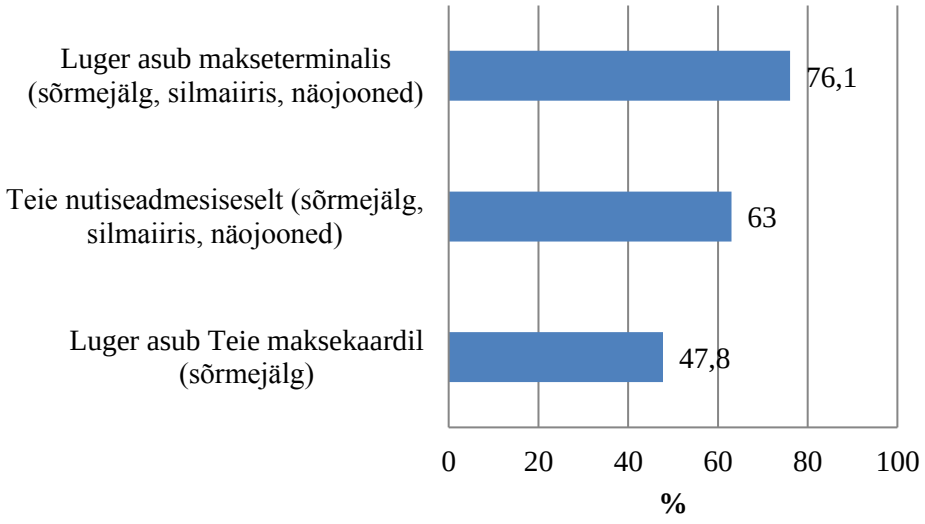


Joonis 13. Kasutamiseks sobilikumad biomeetriliste andmete kandjad protsentides (autori koostatud)

Saadud tulemused näitavad, et inimesed eelistavad meetodi, millest on neil potentsiaalselt parem arusaam või millest võib tekkida ettekujutus selle toimimise

kohta. Küsimuse eesmärk oli uurida, mis oleks tarbija jaoks mugavam kasutamiseks, jättes välja erinevad meetodite detailsed kirjeldused, koos nende eeliste ja puudustega.

Järgmisena oli uuritud, kuidas peaks olema organiseeritud biomeetriliste andmete lugemisprotseduur füüsilises müügikohas (vt joonis 14). Võimaluste valik oli formuleeritud lähtudes varasemalt töös käsitletud teemadest. Lisaks objektidele, mida saab kasutada autentimise protseduuri läbiviimiseks, olid vastavalt välja toodud ka millist biomeetrilist lugemisprotseduuri saab teostada välja toodud valikutes. Kui luger asub maksekaardil, siis ainsaks võimaluseks on kasutada sõrmejälge. Kui luger asub makseterminalis või tarbija nutiseadmes, siis need valikud toetavad sõrmejälge, näojoonte ja silmaiirise autentimist. Kusjuures nutiseadme võimalus tugineb ühele võimalikest mobiilimakse definitsioonidest, mis toetab viipemakse loogikat ning mis lisaks võimaldab ületada viipemakselimiiti, juhul kui autentimine oli tehtud biomeetriliselt. Kuna ühe võimaluse kasutamine ei välista teisi, siis ka antud küsimuse juures sai teha mitu valikut.

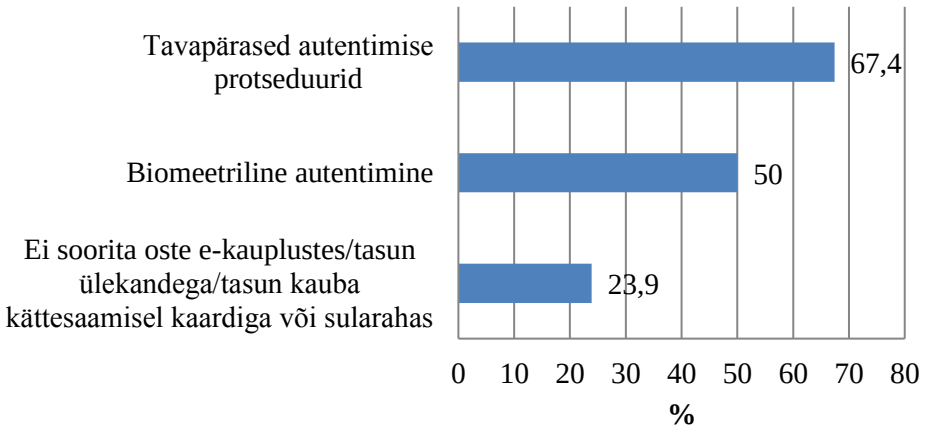


Joonis 14. Biomeetriliste andmete lugemisprotseduuri eelistused füüsilises müügikohas protsentides (autori koostatud).

Vastanute esimeseks valikuks osutus lahendus, mille kohaselt andmete lugemisprotseduur peaks toimuma müügikoha makseterminalis, mida valis 76,1% vastanutest. Hetkel, kõige turvalisemana tunduv lahendus, milleks on sõrmejälje

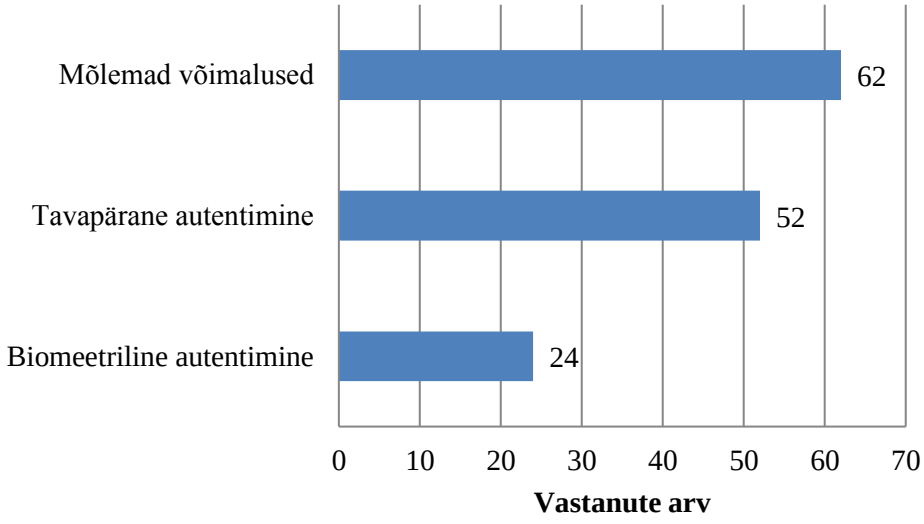
lugeriga pangakaart, on välja pakutud variantidest 47,8%-ga alles kolmandal kohal. Võis oletada, et tehing nutitelefoniga võiks olla populaarsem, eriti arvestades asjaolu, et tegelikult kogu biomeetrilise autentimise protseduur toimub indiviidi oma seadmes, seega omab suuremat kontrolli turvalisuse tagamise kontekstis. Saaks väita, et küllaltki keskmine tulemus on tingitud inimeste kartusest, et nutitelefon, mis oleks turvaline ja töökindel, peab omama teatud funktsionaalsust, mida on võib-olla raske saavutada taskukohase hinnaga ostetud seadmega. Muidugi peab tagama, et nutitelefoni aku oleks laetud, sest vastasel juhul võib vajalikul hetkel vajalik ost tegemata jääda. Siinkohal on oluline märkida, et nutiseadmesisene protseduur ei pea tulema just nutitelefonist, vaid võib tulla ka muust seadmest, mis toetab NFC-tehnoloogiat ning on suuteline biomeetrilisi parameetreid lugema. Selleks sobib ka nutikell või näiteks mõni elektrooniline käevõru. Kokkuvõttes ei saaks ka öelda, et kui lahendusel on 63% toetajaid, siis puudub antud meetodi suhtes huvi. Samas ei saa seda prioritiseerida võrreldes lugeriga, mis asuks makseterminalis. Kuna ükski välja toodud lähenemistest ei välista teist, siis tegelikult saavad nad kõik eksisteerida paralleelselt.

Varasem empiiriline käsitlus, mis puudutas biomeetrilist autentimist Interneti kauplustes näitas üldjoontes, et tegelikult igal lahendusel on omad eelised ja puudused. Biomeetrilise autentimise põhiliseks eeliseks oli selle turvalisus, kuid muudes aspektides võrreldatuna tavapäraste autentimismeetoditega suuri erinevusi ei esinenud. Suhteliselt sarnane tulemus on ka Eesti potentsiaalsete tarbijate eelistustes (vt joonis 15).



Joonis 15. Autentimismeetodi eelistus e-kaubanduses protsentides (autori koostatud).

Selle küsimuse raames sai valida mitme variandi vahel. Põhirõhk on vastustel, mis puudutavad tavapäraseid ja biomeetrilisi autentimise protseduure. Isegi need, kes vastasid, et ei soorita tehinguid Internetikauplustes või tasuvad peale kauba kättesaamist ja mõnda muud viisi kasutades, said valida välja pakutud autentimisprotseduuride vahel, sest sellisel moel saaks teada, kas potentsiaalselt, kui oleksid vastavad võimalused olemas, kas midagi nende eelistustes ka muutuks. Vaadates saadud tulemusi eelistuste lõikes selgus, et neli inimest kes tasuvad kauba kättesaamisel, eelistavad tavapäraseid autentimise protseduure. Veel neli inimest kasutaksid kõiki kolme meetodit, millest võib järeldada, et nende hulgast on tegemist inimestega, kes sooritavad oste Internetikauplustes. Suurem osa vastanutest, kes kas ei kasuta Internetikauplusi või tasuvad kauba kättesaamisel, ei kasuta või ei kasutaks autentimisprotseduure, mis võimaldaksid kaupade või teenuste eest koheselt tasuda. Selliseid vastuseid oli 36. Kuna küsimuses oli eeldatud, et tegemist on tehingu kohese maksega, siis olulisem on vaadelda saadud tulemusi biomeetrilise ja tavapärase autentimise seisukohast (vt joonis 16).



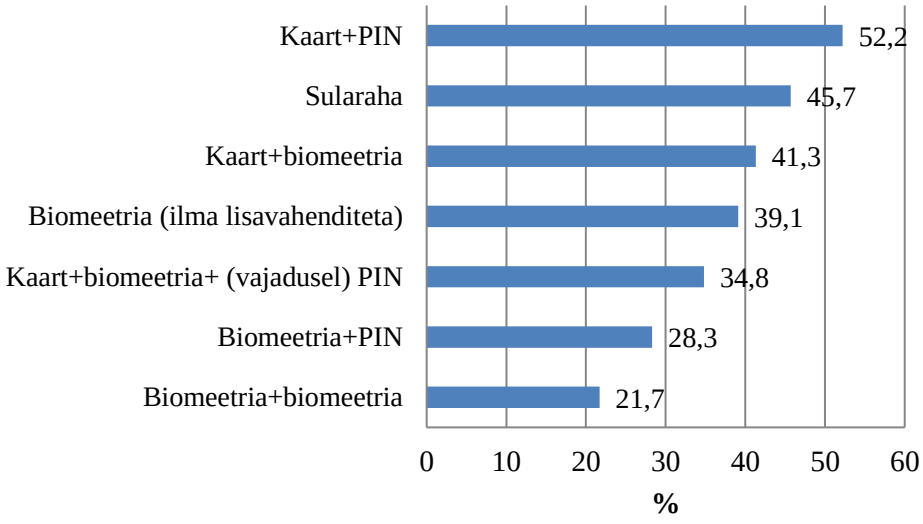
Joonis 16. Internetikauplustes tehingu sooritamise hetkel autentimise meetodite eelistused (in.), autori koostatud.

Välja toodud joonisel on vastanute eelistused autentimise protseduuri läbimisel Internetikauplustes tehingute sooritamisel. Neid, kes pooldasid mõlemat võimalust on 62. Eraldi on välja toodud need vastajad, kes valisid ainut ühe meetodi etteantud

võimaluste hulgast. Selle tulemusena 24 inimest oleksid valmis kasutama ainult biomeetrilist autentimist, samal ajal kui 52 inimest kasutaksid ka edaspidi tavapäraseid autentimisprotseduure. On oluline märkida, et osa nendest, kes sooviksid biomeetrilist autentimist Internetikauplustes on ka nutiseadmesisese biomeetrilise autentimise protseduuri pooldajad. Selline seos esineb 26% vastanute puhul. Sellist madalat numbrit võiks põhjendada sellega, et erinevate müügikoha tüüpide tarbeks läheneksid tarbijad erinevalt.

Antud hetkel saaks järeldada, et kui e-kaubanduses oleks biomeetrilise autentimise funktsionaalsus olemas, siis ta eksisteeriks paralleelselt koos olemasolevate meetoditega.

Teoreetilises osas oli käsitletud biomeetriline autentimine kahe süsteemi seisukohast, millest üks oli verifitseerimise ja teine identifitseerimise süsteem. Selleks, et hinnata biomeetriliste metoodikate potentsiaali ja mida kasutaksid potentsiaalsed tarbijad, oli valimile esitatud küsimust, millised oleksid nende maksemeetodi eelistused (vt joonis 17).



Joonis 17. Maksemeetodi loogika eelistused protsentides (autori koostatud).

Tulemustest selgub, et tavapärane meetod, mille kohaselt kasutatakse PIN-koodiga pangakaarti, on primaarseks eelistuseks. Oli ka neid, kes leidsid, et tulevikus nad loobuksid sularaha kasutamisest, kuid antud hetkel saab järeldada, et teatud põhjustel

on tegemist asendamatu maksevahendiga, kuigi uuringu kontekstis oli tegemist fiktiivse võimalusega, et vastajaid mitte segadusse ajada.

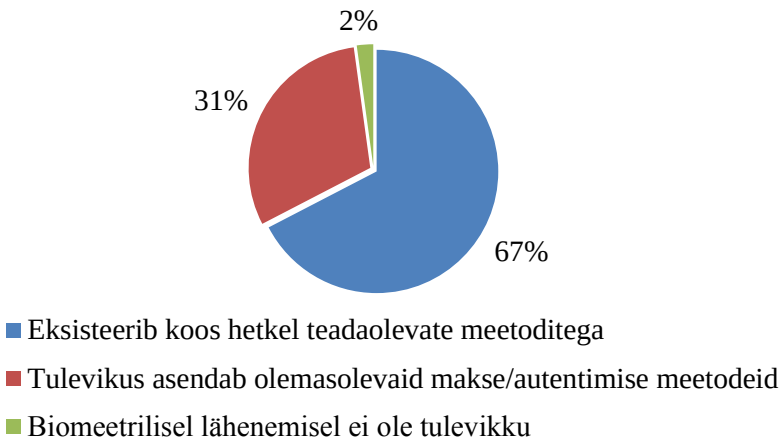
Biomeetrilise verifitseerimise süsteem oli esindatud selliste kombinatsioonidega nagu kaart+biomeetria ja kaart+biomeetria+PIN, kus viimase puhul kaob biomeetrilise autentimise idee juhul, kui andmeid loetakse makseterminalis, mitte kaardi põhjal.

Biomeetriline identifitseerimise süsteem oli esindatud selliste kombinatsioonidega nagu biomeetria ilma lisavahenditeta, biomeetria+PIN ja biomeetria+biomeetria. Viimase variandi kohaselt asendab PIN-i teine objekt, millelt saab biomeetrilisi andmeid lugeda. Näiteks sõrmejäljega loetakse andmeid ja tuvastatakse isik ning teise sammuna kinnitatakse makse näiteks silmaiirisega. Kuna biomeetrilised objektid on ajas muutumatud, siis selline lähenemine vähendaks olulisel määral andmete varastamise riski.

Nagu näitavad tulemused, siis eraldiseisvate lahenduste variantide hulgas sai identifitseerimise süsteemi esindaja kõige väiksema toetuse, kuid sellegipoolest 39,1% vastanutest oleksid lahendusest huvitatud. Verifitseerimise süsteemi populaarsemat lahendust kasutaksid 41,3% vastanutest ning tavapärast meetodit, milleks on PIN-koodiga pangakaart kasutaksid 52,2%. Kui biomeetrilised metoodikad ei oleks eraldi välja toodud, oleksid biomeetriliste meetodite eelistused võrdsed võrreldatuna pangakaardi ja PIN-i võimalusega. Antud küsimuses jäid vaid tavapäraste meetodite juurde vastajad, kes olid nende hulgas, kes algselt ei osanud vastata, kas nad kasutaksid biomeetrilisi meetodeid. Üldjuhul olid vastajad valmis kasutama erinevaid meetodeid.

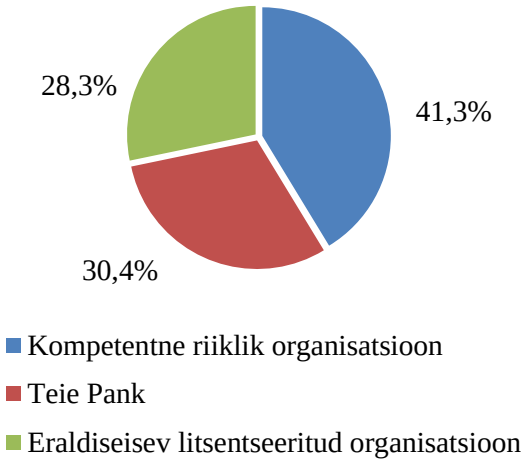
Siinkohal on huvitav teada, milline tulevik võiks olla biomeetrilistel maksetel valimi arvates (vt joonis 18). Maksemeetodi valiku tulemuste kontekstis annab selline hinnang parema ülevaate tarbijate ootuste osas. Ühest küljest võib seda käsitleda kui ootust. Teisest küljest saab seda mõista kui oletusi tuleviku osas. Suurem osa ehk 67% vastanutest arvasid, et tulevikus eksisteerivad biomeetrilised maksed koos hetkel teadaolevate meetoditega. 31% vastanutest julgesid oletada, et biomeetrilised meetodid asendavad hetkel kasutusel olevaid makse- ja autentimsmeetodeid. Osad vastajad, kes oleksid biomeetrilisest lähenemisest huvitatud, leidsid siiski, et tulevikus selliste metoodikate rakendamine on vähetõenäoline. Tulevik on iseenesest lai mõiste ja mingit

kindlat perioodi ei olnud valimi liikmetele välja pakutud, kuid saadud vastused näitavad suhtumist kogu temaatika suhtes.



Joonis 18. Potentsiaalsete tarbijate arvamus biomeetriliste maksete tuleviku osas (autori koostatud)

Rääkides biomeetrilistest andmetest tuleb meeles pidada, et tegemist on sensitiivsete andmetega, mis tähendab, et nende haldus, käitlus ja turvalisuse protseduurid vajavad suurt tähelepanu. Seetõttu oli uuritud, mida arvab valim sellest, kes peaks tegelema nende andmetega (vt joonis 19).



Joonis 19. Biomeetriliste andmete haldaja ja käitleja ning vastutaja (autori koostatud).

Kuna käesoleval hetkel on Eesti riigi halduses inimeste biomeetrilised andmed, siis enne küsitluse läbiviimist võis oletada, et selline oleks ka inimeste eelistus ka maksete kontekstis. 41,3% vastanutest valisidki andmete haldajaks mõnda kompetentset riikliku

organisatsiooni. Osad leidsid, et maksetega seonduv peaks olema panga vastutusalas ja seda soovis 30,4% vastanutest. 28,3% valimist leidsid, et kogu selle temaatikaga peab tegelema eraldiseisev litsentseeritud organisatsioon. Eraldiseisev organisatsioon oleks hea valik, sest siis oleks tegemist organisatsiooniga, mis tegeleks ainult antud temaatikaga, mis peaks vastama erinevate osapoolte regulatsioonidele. Samas arvestades seda, et isikut tõendavad dokumendid sisaldavad biomeetrilisi andmeid, võiksid ka edaspidised biomeetrilised toimingud olla riigi halduses.

Saaks oletada, et juhul kui oleks tehtud asjakohane ja mitmekülgne teavitustöö ning oleks ka võimalus biomeetrilise süsteemi toimimist demonstreerida, siis ka küsitluse vastused erineksid.

Antud temaatikas kasutavad inimesed seda, mida on võimalik kasutada või seda, mida luuakse ja pakutakse. Näiteks võib välja tuua kaardiga tehtavaid viipemakseid. Kui seda võimalust ei olnud, siis inimesed ei osanud seda ka soovida. Nüüd, kui see funktsionaalsus on olemas, siis seda saab kasutada või mitte. Turvariskide maandamiseks saab selle funktsionaalsuse ka deaktiveerida. Sama olukord on ka biomeetriliste maksetega. Maksete valdkonnas otsitakse ja luuakse innovatiivseid lahendusi, mis muudaksid tehingute sooritamist kiiremaks, mugavamaks ja turvalisemaks. Nagu varasemalt sai mainitud, tahavad suuremad autoriseerimisvõrgud muuta kohustuslikuks biomeetrilist autentimist toetavate kaartide vastuvõtu. See on esimeseks sammuks biomeetriliste perspektiivide jaoks maksete valdkonnas.

Tehtud uuringu põhjal saab väita, et potentsiaalsed tarbijad oleksid huvitatud biomeetrilistest maksetest, mida saaks kasutada paralleelselt koos hetkel teadaolevate maksemeetoditega. Biomeetriliste maksete potentsiaalne kasutaja jääb vanuse vahemikku 18-55 eluaastat, kelle eelistus maksemeetodi valikul on pangakaart. Need kasutajad eelistaksid, et andmeid saaks lugeda sõrmejäljelt ning luger võib vastavalt eelistusele asuda makseterminalis, nutiseadmes või maksekaardil ning andmete haldus võiks toimuda riikliku organisatsiooni poolt. Samuti esineb huvi biomeetriliste meetodite vastu e-kaubanduse valdkonnas ning teatud segment kasutaks tehingute teostamiseks oma nutitelefoni. Inimesed on avatud biomeetriliste maksemeetodite tulekuks, kuid vajavad rohkem informeeritust selle olemuse, eeliste ja puuduste osas. Ei

ole ka välistatud biomeetrilise identifitseerimise süsteemi loogika kasutus, kuid selline lahendus peab olema mitmekülgselt läbi mõeldud.

KOKKUVÕTE

Maksemeetodite valdkond on suur, mitmekesine, rangelt reglementeeritud ja sügavalt uurides ka keerulise ülesehitusega koos oma võimaluste ja ohtudega. Tehnoloogia arenguga tekib palju uusi võimalusi innovaatiliste lahenduste kasutusele võtmiseks, mis avaldab mõju finantsteenuste valdkonnale, luues eeliseid progressiga kaasa minejatele. Tegemist on valdkonnaga, mis peab järjekindlalt arenema eesmärgiga tagada klientidele paremat turvalisust, kiirust ja mugavust oma igapäevaste toimingute teostamiseks. Igapäevaselt puutuvad inimesed kokku müügikohtades tehingute teostamisega, mis muudab antud temaatikat aktuaalseks ja atraktiivseks erinevate osapoolte jaoks. Biomeetriline lähenemine oleks üks võimalikest tuleviku väljavaadetest antud valdkonnas.

Käesoleva bakalaureusetöö eesmärgiks oli selgitada potentsiaalsete tarbijate huvi biomeetriliste maksete suhtes Eestis. Eesmärgi saavutamiseks olid teoreetilises osas põhjalikult käsitletud biomeetrilise autentimise olemust ja maksemeetodeid ning toimimisloogikat, mida kasutatakse Eestis müügikohtades arveldamisel ning on lähtutud meetodite omavahelise integratsiooni seisukohast.

Biomeetrilist autentimist vaadeldakse kui tuvastusmeetodi järgmist generatsiooni, mille andmekandjad on igal inimesel unikaalsed ning seda peetakse turvalisemaks võrreldes alternatiivsete seni teadaolevate autentimismeetoditega. Biomeetrias eristatakse kaht põhilist autentimise süsteemi loogikat, milleks üks on verifitseerimise ja teine identifitseerimise süsteem. Verifitseerimise süsteemis toimub „üks-ühele“ tuvastus, mis on võrreldav protseduuriga, mis kasutaks kasutajatunnust ja parooli, kus biomeetrilised parameetrid asendavad parooli osa. Identifitseerimise süsteemis toimub „üks-mitmele“ tuvastus, kus süsteem otsib täpset vastet konkreetsele kasutajale mitme kasutaja hulgast

ja ei eelda lisavahendi olemasolu protseduuri teostamiseks ehk meetod, mis justkui kasutaks ainult parooli. Biomeetrilise tuvastusprotseduuri läbimiseks on olemas eeldused, mis peavad olema täidetud, et lahendus saaks toimida. Teoreetilisteks eeldusteks on universaalsus, mis tagab, et igal indiviidil peab olema vajalik tunnus; unikaalsus , mis garanteerib, et tunnused ei katu; püsivus, mis vastutab selle eest, et tunnus aja jooksul ei muutu; kogumisvõime, mis tähendab, et tunnuseid saab mõõta kvantitatiivselt. Praktilisteks eeldusteks on toimimine, mis tähendab korrektsete tulemuste saavutamiseks vajalikke ressursside ja tingimuste olemasolu; vastuvõetavus, mis määrab ära kuivõrd on kasutajad selle kasutamiseks valmis; möödahiilimine, mis vastutab selle eest, et süsteemi oleks võimalikult keeruline petta.

Biomeetrilisi andmeid saab lugeda mitmelt erinevalt objektilt, kuid iga võimalus maksete konteksti ei sobi. Selleks, et oleks tegemist maksimaalselt sujuva ja turvalise protsessiga oli käesolevas uuringus võimaluste arv minimeeritud kolmele. Arvestades teoreetilisi eeldusi ning et tegemist on tehingutega müügikohas ja kombineerides teoreetilisi seisukohti olid valitud protseduurid, mille kohaselt loeti andmeid sõrmejäljelt, silmaiiriselt ja näolt.

Biomeetriliste meetodite integreerimine tavapärastesse maksemeetoditesse viib huvitava järelduseni. Nimelt biomeetrilise verifitseerimise süsteemi kohaselt, toimib kõik tuginedes tavapärasele kaardimakse loogikale, kus biomeetriline aspekt on kasutuses vaid autentimise protseduuri teostamiseks. Biomeetrilise identifitseerimise süsteemi kohaselt on aga teoreetiliselt võimalik toetuda muule loogikale, jättes välja tavapärased maksete toimimismehhanismid. Sellise lähenemise puhul, biomeetriline lähenemine on võimeline tõrjuma seni teadaolevaid maksemeetodite toimimisloogikat. Mobiilimaksed on teinud suure arengu ning on olemas mitmeid definitsioone, mis kirjeldavad üht või teist makse teostamise protseduuri ja olenemata sellest, mis käsitluse kohaselt mobiilimakseid vaadelda, on biomeetriline meetod teoreetiliselt rakendatav mõlema tuvastussüsteemi korral. Sarnane olukord on ka e-kaubandusega, mis on arenenud tänu Interneti ajastule. Siinkohal esineb aga piirang kuna tegemist pole füüsilise müügikohaga, võib potentsiaalne turvarisk suureneda, sest Internetis on rohkem võimalusi juhuslikult oma andmete lekitamiseks. Samas kui ostelda Internetis kasutades oma nutiseadet, mis on biomeetrilise toega, on see risk minimeeritud. Biomeetrilise

identifitseerimise süteemi teoreetiline rakendamine tähendaks struktuurseid ja massilisi muutusi tehingute liikumise taristus. Toetudes varasematele tavapraktika teoreetilistele käsitlustele, pakkus käesoleva töö autor välja meetodi, mis võiks toimida.

Empiirilises osas, esimeses alapeatükis, leidsid kinnitust mõned teoreetilised seisukohad, mis viitasid asjaolule, et biomeetrilise autentimise alused on ajas muutumatud ja loeb vaid käesoleva hetke tehnoloogiaareng ja ressurssid. Tuvastusprotseduuri täpsus ja turvalisus sõltub valitud algoritmist ning kasutatavast tark-ja riistvarast. Sõrmejäle, silmaiirise ja näo tuvastustehnoloogia omavad suurepäraseid omadusi ning on selge, et on võimalik saavutada maksimaalne tulemus. See ei tähenda aga, et seda saab saavutada iga inimene või ettevõte, kes otsustab antud valdkonnas tegutseda. Huvi biomeetriliste metoodikate kasutamise vastu maksemetodites on olnud viimastel aastatel suur. On tehtud erinevaid uuringuid, pilootprojekte ja küsitlusi. Adekvaatsed teaduslikud empiirilised uuringud, mis puudutavad konkreetselt makseid, piirduvad üldjuhul ankeetküsitlustega või vaatlusega. Käesoleva töö autor selgitas välja, millega peaks arvestama näiteks biomeetrilise makseterminali prototüübi loomisel, et saavutada maksimaalne võimalik tulemus uuringu tegemisel. See teekond on väga keeruline ja ressurssinõudev ning peab vastama mitmele standardile. Arvestades sellega, et sellise katse tegemiseks kasutatakse inimeste sensitiivseid andmeid, mis on staatilise loomuga, ei ole eetiline teostada selliseid katseid standarditele mittevastava lahendusega. Biomeetrilist autentimist on uuritud ka e-kaubanduse raames, mille tarbeks olid loodud testandmed ja selle tulemused viitasid sellele, et biomeetrilised meetodid oleksid kasutusel koos seniteadaolevate meetoditega, sest kasutajad leidsid, et lahendusel on omad eelised, aga kohati teatud tingimustes mitte nii märkimisväärsed.

Tuntumad autoriseerimisvõrgud, milleks on Mastercard ja Visa, on aktiivselt biomeetriliste maksete valdkonnaga tegelenud. Nad on teinud erinevaid uuringuid ja koostanud vajalikke spetsifikatsioone. See toimus sellel taustal, et juba on loodud pangakaart, millesse on sisseehitatud sõrmejälje luger. Lähimas tulevikus kohustatakse müügikohti ja koos nendega ka pankasid, et selliste kaartide vastuvõtmine oleks võimaldatud. Sellest saab valdkonna biomeetrilise arengu alguseks. Antud juhul, tänu oma turuosale, autoriseerimisvõrgud dikteerivad oma tingimusi maailmale.

Identifitseerimissüsteemi tulekuga võivad jõujooned aga muutuda. Kõik oleneb sellest, kas selline lahendus on tulevikus võimalik ja kes sellega tegelema hakkab.

Empiirilise osa teises alapeatükis oli presenteeritud autoripoolse uuringu tulemused, mille eesmärgiks oli selgitada potentsiaalsete tarbijate huvi biomeetriliste maksete suhtes Eestis. Selle tarbeks oli läbiviidud ankeetküsitlus. Mitmekülgse analüüsi tegemiseks olid küsimused koostatud tuginedes teoreetilisele baasile ja varasematele empiiriliste uuringutele. Valimis oli 220 Eestis elavat täisealist isikut. Uuringu tulemused näitasid, et huvi biomeetriliste lahenduste suhtes on olemas. Ligi 60% vastanutest on selgelt väljendanud soovi, et maksed saaksid toimida biomeetriliselt. Ligi veerand ei osanud oma huvi hinnata, kuid siiski väljendasid oma seisukohti, kuidas peaks potentsiaalne biomeetriline makseprotseduur olema organiseeritud. 16,4% vastanutes olid suhtunud sellesse negatiivselt. Alates 55. aastasest vanusest olid suurem osa vastanutes suhtunud negatiivselt, nagu ka need, kelle maksemeetodi eelistuseks on sularaha. Üldiselt saab järeldada, et huvi biomeetriliste maksete suhtes on suur, kuid nad saaksid eksisteerida paralleelselt olemasolevate autentimis- ja maksemeetoditega ja seda meelt olid 67% vastanutest. 31% leidsid, et tulevikus biomeetrilised meetodid asendavad olemasolevaid meetodeid turult. Oluline on välja tuua, et tarbijad on huvitatud nii biomeetrilise verifitseerimise kui ka identifitseerimise süsteemi lähenemisloogikast. Identifitseerimissüsteemi toetust, saab hinnata mitte ainult makseviisi eelistuste valikutest lähtudes, vaid ka küsimusest, mis puudutas vastutust biomeetriliste andmete turvalisuse ja käitlemise osas. Selle kohaselt 41,3% vastanutest arvasid, et tegemist võiks olla riikliku organisatsiooniga. 30,4% usaldaksid need protsessid oma panga kätte ja 28,3% vastanutest eelistaksid, et sellega tegeleks eraldiseisev litsentseeritud organisatsioon. Kokkuvõtvalt saaks järeldada, et esialgu oleks huvi tasuda oma toodete ja teenuste eest biomeetriliselt nii füüsilises, kui ka Internetipõhises müügikohas. Andmete lugemine võiks toimuda makseterminalipõhiselt, kuid ka oma nutiseadmepõhiselt, kasutades selleks eelkõige sõrmejälge.

Bakalaureusetöö eesmärk sai täidetud- potentsiaalsete tarbijate huvi biomeetriliste maksete suhtes Eestis on välja selgitatud. Tarbijate huvi biomeetriliste maksete vastu on olemas. Püstitatud ülesanded eesmärgi saavutamiseks aitasid läheneda

uurimisprobleemile mitmekülgselt ning välja selgitada ka võimalikke tuleviku perspektiive. Keeruline on väita, et saadud tulemusi saab üle kanda üldkogumile, kuid annab selge ülevaate antud teema potentsiaalist. Üldkogumile üldistamiseks peab potentsiaalsed biomeetrilise maksemeetodi kasutajad olema rohkem informeeritud ning valimi maht võiks olla suurem, mis oleks võimalik tingimustes, kus inimestel oleks juba uuringu hetkeks olemas piisav informatsioon ja biomeetrilist autentimist toetavate lahenduste minimaalne kasutamise kogemus. Teema edasiarendamise võimaluseks on käsitleda antud teemat rohkem biomeetrilise identifitseerimise süsteemi seisukohast hinnates võimalikku mõju pankadele ja autoriseerimisvõrkudele. Antud töö on ka abiks praktiliste lähenemiste organiseerimiseks.

VIIDATUD ALLIKAD

1. 3-D secure. Mastercard. [https://www.mastercard.com/gateway/implementation_ guides/3D-Secure.html]. 03.11.2016.a.

2. 90% of Dutch shoppers prefer biometrics to passwords. Biometric Technology Today. 2016, Iss 3, 03.2016, pp. 2 . DOI: [http://dx.doi.org.ezproxy.utlib.ut.ee/10.1016/S0969-4765(16)30042-X]

3. Abbasi, A., Seng W.C., Unar, J.A. A review of biometric technology along with trends and prospects.- Pattern Recognition. Elsevier, 2014, Iss.47 pp. 2673–2688

4. Adamek, M., Matysek, M., Neumann, P. Security of Biometric Systems. - Procedia Engineering. Elsevier, 2015, Vol. 100, pp 169–176.

5. Aguilar, D., Ibarra, L., Partida, A. Electronic commerce as a business strategy: Impact in consumption habits in Hermosillo, Sonora's inhabitants. -Procedia - Social and Behavioral Sciences. Elsevier. 2015, Vol. 175, pp. 275 – 282.

6. Ahuja, V., Khazanchi, D. Creation of a conceptual model for Adoption of Mobile Apps for shopping from E-Commerce sites-An Indian context. -Procedia Computer Science. Elsevier. 2016, Vol. 91, pp. 609 – 616.

7. Arévalo, J., Gómez, J,A., Nin, J., Paredes, R. End-to-end neural network architecture for fraud scoring in card payments. -Pattern Recognition Letters, 2017, 7 p. DOI: [http://dx.doi.org/10.1016/j.patrec.2017.08.024]

8. Ashrafi, M, Z., Ng, S, K. Privacy-preserving e-payments using one-time payment details.- Computer Standards & Interfaces. Elsevier, 2009, Vol. 31, Iss. 2, pp 321-328.

9. Bolle, R., Hong, L., Jain A.K., Pakanti, S. An Identity-Authentication System Using Fingerprints.- Proceeding of the IEEE, Vol.85 No.9, 1997, pp 1365-1388.

10. Breebaart, J., Buhan, I., Groot, K., Kelkboom, E. Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment

infrastructure. -Electronic Commerce Research and Applications. Elsevier, 2011, Vol. 10, pp. 605-614.

11. Clodfelter, R. Biometric technology in retailing: Will consumers accept fingerprint authentication? -Journal of Retailing and Consumer Services. 2010, Vol. 17, pp. 181–188.

12. Cocosila, M., Trabelsi, H. An Integrated Value-Risk Investigation of Contactless Mobile Payments Adoption.-Electronic Commerce Research and Applications. Elsevier, 2016, p 45.

13. Coetzee, M. Advanced biometric technology: Reinforcing security within payment systems.- Journal of Payments Strategy & Systems. 2013, Vol. 7, No. 1, pp 73-89.

14. EMVCo, URL: [https://www.emvco.com/about/overview/] 16.02.2018

15. European consumers ready to use biometrics for security payments. Visa Europe, 2016, 2 p, URL: [https://www.visaeurope.com/media/pdf/37840.pdf] 29.10.2016.a.

16. French banks, retailers to pilot biometric payment method. Biometric Technology Today. 2012, Iss 10, 2 p. DOI: [http://dx.doi.org.ezproxy.utlib.ut.ee/10.1016/S0969-4765(12)70194-7]

17. Google Pay. URL: [https://pay.google.com/about/] 27.03.2018.a.

18. Gurvirender P. T., Zareef A. M. Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals' perceptions toward technology.- Computers & security. Elsevier, 2017, Vol. 67, pp. 254–265.

19. Hess, T., Köster, A., Matt, C. Carefully choose your (payment) partner: How payment provider reputation influences m-commerce transactions. -Electronic Commerce Research and Applications. 2016, Vol 15, pp. 26–37.

20. Jain, A.K., Nandakumar, K., Ross, A. 50 years of biometric research: Accomplishments, challenges, and opportunities.- Pattern Recognition Letters, 2016 Vol. 79 pp. 80–105.

21. Jain, A.K., Prabhakar, S., Ross, A. An Introduction to Biometric Recognition.- Transactions on Circuits and Systems for Video Technology, Vol.14, Iss.1, 2004, pp 4-20.

22. Khalid, H., Mun, Y, P., Nadarajah, D. Millennials' Perception on Mobile Payment Services in Malaysia. -Procedia Computer Science. 2017, Vol. 124, pp. 397–404.

23. Kim, D.J., Ogbanufe, O. Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. -Decision Support Systems. Elsevier. 2018, Vol. 106, pp 1–14.

24. Kim, H.J. Biometrics, is it a viable proposition for identity authentication and access control? -Computer Security. 1995, Vol 14 pp 205–214.

25. Kleist, V.F. Building technologically based online trust: can the biometrics industry deliver the online trust silver bullet? -Information Systems Managagement. 2007, Vol. 24. Iss 4. pp. 319–329.

26. Korolev, A., Krivosheya, E. Benefits of the retail payments card market: Evidence from Russian merchants. -Journal of Business Research. Elsevier. 2017, 8 p, DOI: [https://doi.org/10.1016/j.jbusres.2017.12.020]

27. Lara-Rubio, J., Liébana-Cabanillas, F. Predictive and explanatory modeling regarding adoption of mobile payment systems. -Technological Forecasting & Social Change. 2017, Vol. 120, pp. 32–40.

28. Lumini, A., Nanni, L. Overview of the combination of biometric matchers. -Information Fusion. Elsevier, 2017, Vol. 33, pp.71–85.

29. MasterCard and Visa look to upgrade payment security with biometrics.- Biometric Technology Today. Elsevier, 2015, Iss.1, 11 p, DOI: [https://doi.org/10.1016/S0969-4765(15)70015-9]

30. Mastercard and Visa make major push with biometric cards. -Biometric technology today, DOI: [https://doi.org/10.1016/S0969-4765(18)30015-8]

31. Mastercard Customer Interface Specification.- Mastercard. 2010, 874 p, URL: [https://kupdf.com/download/customer-interface-specification_58713fb86454a7af1035c073_pdf] / URL: [www.mastercardconnect.com]

32. Mastercard Transaction Processing rules.– Mastercard. 2017, p 296, URL: [file:///C:/Users/Olev/Downloads/transaction-processing-rules%20(2).pdf]

33. Nets Payment System Messaging Standard. 2017, 68 p, URL: [https://www.estcard.ee/standards/emv/Messaging_standard_5.61.0.pdf]

34. Normalini, M.K., Ramayah, T. Biometrics Technologies Implementation in Internet Banking Reduce Security Issues? -Procedia - Social and Behavioral Sciences. Elsevier. 2012, Vol 65, pp. 364 – 369.

35. PCI SSC Data Security Standards Overview. URL: [https://www.pcisecuritystandards.org/pci_security/standards_overview] 18.02.2018.a.

36. Phillips, P. J., Scruggs, W. T., OToole, A. J., Flynn, P. J., Bowyer, K. W., Schott, C. L, Sharpe, M. FRVT 2006 and ICE 2006 large-scale results. Technical Report, NISTIR, 2007. p 55, URL: [http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=51131] 04.02.2017.a.

37. Przybocki, M., Martin, A. NIST speaker recognition evaluation chronicles. In Odyssey: The Speaker and Language Recognition Workshop, Toledo, Spain, 05.2004, pp 12-22, URL: [https://www.nist.gov/itl/iad/IADpapers/2004/ABSFBE1562.pdf] 10.01.2017.a.

38. Smart ID. URL: [https://smartid.ee/what/] 10.01.2018.a.

39. Sokolowska, E. Innovations in the payment card market: The case of Poland. -Electronic Commerce Research and Applications. Elsevier. 2015, Vol. 14, pp.292-304.

40. Sõrmejäljega tehingute kinnitamine.- Pocopay. URL: [https://pocopay.com/uuendused/sormejaljega-tehingute-kinnitamine/] 05.10.2016.a.

41. Vessem, I. EMV in transit: What are these EMV Level 1, 2, 3 Certifications.- UL Transaction Security Blog. 2017, URL: [https://blog.ul-ts.com/posts/emv-in-transit-what-are-these-emv-level-1-2-3-certifications/]

42. Visa Dual Message System Authorization (DMSA) Processing Specifications. -Visa Online. 2015, p 188, URL: [https://www.visaonline.com/login/LoginMain.aspx?goto=https%3A%2F%2Fsecure.visaonline.com%3A443%2F]

43. Visa Core Rules and Visa Product and Service Rules. -Visa Europe, 2017, 876 p, URL: [https://www.visaeurope.com/media/images/visa%20core%20rules%20and%20visa%20product%20and%20service%20rules%202017-73-40575.pdf]

44. Ward, M. EMV card payments – An update. -Information Security Technical Report. Elsevier, 2006, Vol. 11, Iss. 2, pp 89-92.

45. Wayman, J.L. The scientific development of biometrics over the last 40 years, in The History of Information Security: A Comprehensive Handbook. Elsevier, 2007, pp 263–274.

46. Wilson, C., Hicklin, A. R., Bone, M., Korves, H., Grother, P., Ulery, B., Micheals, R., Zoep, M., Otto, S., Watson, C. Fingerprint vendor technology evaluation 2003: summary of results and analysis report. Technical Report NISTIR, 2004. URL: [https://www.nist.gov/itl/iad/image-group/fingerprint-vendor-technology-evaluation-fpvte-2003] 04.02.2017.a.

LISAD

Lisa 1. Biomeetriliste mõõtmisobjektide omadused

Biomeetriline objekt	Universaalsus	Eristusvõime	Püsivus	Kogutavus	Esitus	Vastuvõetavus	Möödahiilimine
DNA	Kõrge	Kõrge	Kõrge	Madal	Kõrge	Madal	Madal
Kõrv	Keskmine	Keskmine	Kõrge	Keskmine	Keskmine	Kõrge	Keskmine
Nägu	Kõrge	Madal	Keskmine	Kõrge	Madal	Kõrge	Kõrge
Näo termo-gramm	Kõrge	Kõrge	Madal	Kõrge	Keskmine	Kõrge	Madal
Sõrmejälg	Keskmine	Kõrge	Kõrge	Keskmine	Kõrge	Keskmine	Keskmine
Kõnnak	Keskmine	Madal	Madal	Kõrge	Madal	Kõrge	Keskmine
Labakäe geomeetria	Keskmine	Keskmine	Keskmine	Kõrge	Keskmine	Keskmine	Keskmine
Käe veenid	Keskmine	Keskmine	Keskmine	Keskmine	Keskmine	Keskmine	Madal

Silmaiiris	Kõrge	Kõrge	Kõrge	Keskmine	Kõrge	Madal	Madal
Klahvi-vajutus	Madal	Madal	Madal	Keskmine	Madal	Keskmine	Keskmine
Lõhn	Kõrge	Kõrge	Kõrge	Madal	Madal	Keskmine	Madal
Peopesa	Keskmine	Kõrge	Kõrge	Keskmine	Kõrge	Keskmine	Keskmine
Võrkkest	Kõrge	Kõrge	Keskmine	Madal	Kõrge	Madal	Madal
Allkiri	Madal	Madal	Madal	Kõrge	Madal	Kõrge	Kõrge
Hääl	Keskmine	Madal	Madal	Keskmine	Madal	Kõrge	Kõrge

Allikas: Jain *et al* 2004:11

Lisa 2. Küsimustik

Biomeetriliste maksete rakendusperspektiivid Eestis

Küsitluse eesmärgiks on välja selgitada potentsiaalsete tarbijate huvi biomeetriliste maksete suhtes Eestis. Kokku on 10 küsimust. Küsimustele vastamine võtab aega umbes 5-10 minutit. Tänan Teid ette, et leidsite aega küsimustikule vastamiseks!

1. Märkige palun oma vanus.

   _____

2. Kas Te olete varasemalt kokku puutunud biomeetrilise autentimise temaatikaga (kasutanud/uurinud/lugenud/kuulnud)?

   a) Jah ☐ b) Ei ☐

3. Milline on Teie maksemeetodi eelistus toodete või teenuste eest tasumisel müügikohas ? Valida üks.

   a) Pangakaart ☐ b) Sularaha ☐

4. Biomeetriline autentimine (käesolevas kontekstis) on isiku autentimine, kasutades selleks indiviidi unikaalseid füsioloogilisi omadusi (nt. sõrmejälg, silmaiiris, näojooned). Kui Teil oleks võimalus tasuda biomeetriliselt, siis kas Te kasutaksite sellist võimalust?

   a) Jah ☐ b) Ei ☐ c) ei oska öelda ☐

   (Kui Te valisite „Ei“, siis ei pea järgnevatele küsimustele vastama)

5. Millelt on biomeetriliste andmete lugemine Teie arvates mugavam/sobilikum (võib valida mitu):

   a) Sõrmejälg ☐
   b) Silmaiiris ☐
   c) Näojooned ☐

6. Kuidas peaks Teie arvates olema ära lahendatud biomeetriliste andmete lugemisprotseduur füüsilises müügikohas maksetehingu sooritamisel (võib valida mitu)?

   a) Biomeetriliste andmete luger/skänner on makseterminalis (sõrmejälg,silmaiiris,näojooned) ☐
   b) Luger asub Teie maksekaardil (sõrmejälg) ☐
   c) Teie nutiseadmesiseselt (nt. nutitelefon), millega saab sooritada tehingut viipemakse loogika alusel, kui oleks võimalik tänu biomeetrilisele meetodile ületada viipemakselimiidi piirangut. (sõrmejälg, nägu, silmaiiris) ☐

7. Internetikauplustes ostude sooritamiseks kasutaksite (võib valida mitu):

   a) Tavapäraseid autentimise protseduure ☐
   b) Biomeetrilist autentimist ☐
   c) Ei soorita oste e-kauplustes/tasun ülekandega/tasun kauba kättesaamisel kaardiga või sularahas ☐

8. Millise maksemeetodi loogikat kasutaksite tulevikus(võib valida mitu)?

   a) Kaart+PIN ☐
   b) Kaart+biomeetria ☐
   c) Kaart+biomeetria+ (vajadusel) PIN ☐
   d) Biomeetria (ilma lisavahenditeta) ☐
   e) Biomeetria+PIN ☐
   f) Biomeetria+biomeetria(tehingu kinnitamiseks) ☐
   g) Sularaha ☐

9. Milline tulevik on Teie arvates biomeetrilistel maksetel (valida üks)?

   a) Tulevikus asendab olemasolevaid makse/autentimise meetodeid ☐
   b) Biomeetrilisel lähenemisel ei ole tulevikku ☐
   c) Eksisteerib koos hetkel teadaolevate meetoditega ☐

10. Kes peaks Teie biomeetrilisi andmeid haldama, käitlema ja vastutama turvalisuse eest (valida üks)?

    a) Teie Pank ☐
    b) Kompetentne riiklik organisatsioon ☐
    c) Eraldiseisev litsentseeritud organisatsioon ☐

Suur tänu vastamise eest!

SUMMARY

PERSPECTIVES ON THE IMPLEMENTATION OF BIOMETRIC PAYMENTS IN ESTONIA

Olev Gudovski

The rapid technological development that covers different areas is also the reason why a bigger attention is required in the topic of usable payment methods. The area of payments is large, diversified and inclusive. To a large extent, transactions are carried out at various points of sale on a daily basis. Payment methods and their preferences at points of sale are part of the financial services category. The development of financial services is, in turn, dependent on a sector that creates innovative financial solutions (Sokolowska 2015: 292). Along with innovative solutions, the financial services market is developing, which in turn has a positive impact on the economy.

The speed, convenience and security of a payment transaction are three of the key indicators that need to improve continuously. If this area were not to be sustained, it would be easier for criminals to invent methods for misusing foreign means of payment. The development of payment options will stimulate competition across sectors and can provide an edge for those who are involved with the development process.

In the author's view, the next possible step in the development of payment methods could be biometric payments, whose partial potential has already been used today. Publicly, this topic hasn´t been investigated in Estonia. One might assume that its causes are related to concepts such as business secrets, corporate business strategy, etc. Biometric payments have previously been investigated as a payment confirmation tool. Indeed, when talking about biometric payment, in particular, biometric authentication is

considered, which in this context would mean confirmation of payment using a biometric method that would replace traditional methods such as a PIN or password entry according to the type of point of sale. The advantage of the entire method lies in the fact that it is something that you do not have to remember or carry with you separately.

Card payments are a fundamental basis for innovative and modern payment methods. This is a safer and faster payment method compared to using cash (Korolev and Krivosheya 2017: 2). Linking a biometric solution with the card payment logic, is one of the possible approaches in the given field. On the other hand, theoretically, a biometric method can also be considered as a payment method, which would not require the use of additional resources, besides only the mere reading of biometric data, which could also be called a direct biometric payment and it would be sufficient to complete the transaction.

The aim of this Bachelor's thesis was to identify the interest of potential consumers in using biometric payments in Estonia. For achieving the goal the following research tasks were arisen:

• consider the nature of the biometric authentication and its appropriate methods for using in payments,

• consider the content and operational logic of payment methods currently used, based on scientific literature,

• provide an overview of the possible integration of biometric methods with available payment methods based on a scientific literature.

• provide an overview of the nature of the biometric payment based on the biometric authentication and known payment processing mechanism,

• create a questionnaire based on theoretical approach and from previous empirical studies and conduct a survey among private payers,

• analyze the results obtained and draw conclusions with the author's assessment of the implementation and development of biometric payment methods

Biometric authentication is considered to be the next generation of authentication method. The identifiers, which are unique to each individual are considered to be safer for usage compared to alternative authentication methods that are known so far. Biometrics autehntication possible approach is divided between two basic authentication system logics, one of which is the verification and the other, the identification system. In the verification system there is a "one-on-one" matching that is comparable to a procedure that uses a user name and a password where biometric parameters replace the password part. In the identification system, an "one-to-many" matching occurs where the system searches for exact matches for a particular user from multiple users and does not require additional tools for performing a procedure, that is for example a method, that just uses a password. There are assumptions that must be made to complete the biometric authentication procedure in order for the solution to work. The theoretical assumptions are universality, which ensures that each individual has the necessary identifier; uniqueness, which ensures that the identifier features do not cover; persistence, which is responsible for ensuring that the identifier feature does not change over time; collectablity, which means that the characteristics can be measured quantitatively. Practical prerequisites are the operation, which means the availability of resources and conditions necessary to achieve the correct results; acceptability, which determines how users are ready to use it; passing by, which is responsible for making the system as complex as possible to deceive. The most suitable biometric identifiers in the filed of payments are fingerprint, iris and face recognition.

Integrating biometric methods into standard payment methods leads to an interesting conclusion. Namely, according to the biometric verification system, all operate on the basis of the usual card payment logic, where the biometric aspect is used only for the authentication procedure. However, according to the biometric identification system, it is theoretically possible to rely on a different logic by eliminating the usual payment mechanisms. In this approach, a biometric approach is capable of deflecting the well-known payment methods logic. Mobile payments have made great progress and there are a number of definitions that describe one or another payment execution procedure and regardless of which mobile payment is considered, the biometric method is theoretically applicable to both systems of authentication. A similar situation is with e-commerce, which has evolved thanks to the Internet era. However, there is a restriction

here, since this is not a physical point of sale, the potential security risk may increase. But while shopping on the Internet using your smartphone, which handles the payment procedure biometrically, then this risk is minimized. The theoretical implementation of the biometric identification scheme would mean structural and massive changes in the transaction flow infrastructure. Based on previous theoretical approaches to standard practice, the author proposed a method that could work on the basis of biometric identification system.

The basics of biometrics remains the same through time and only thing to consider is the technological development of the given moment and its opportunities and the resources that are used. The accuracy and security of the recognition procedure depends on the chosen algorithm and the software and hardware used. Fingerprint, iris, and face recognition technologies have great features and it's clear that achieving maximum results in accuracy and security are possible. Various studies, pilot projects and surveys have been previously carried out. Adequate scientific empirical studies specifically relating to payments with biometrical approach are generally limited to questionnaires. The author of this paper explains what should be considered, for example, in creating a prototype of a biometric payment terminal in order to achieve the maximum possible result for the study in investigating the interest of the potential users by using a prototype . This route is very complicated and resource-intensive and must meet several standards. Using sensitive data which has a static nature, is not ethical to carry out such experiments with a non-standardized solutions. The most well-known authorization networks, namely Mastercard and Visa, have been active in the area of biometric payments. They have done various research and produced the necessary specifications. They have set requirements for the banks and merchants to be ready for accepting payments which use biometric verification in the nearest future. This will be the beginning of biometric development in the field. In this case, due to their market share, authorization networks dictate their conditions to the world. However, force lines may change with the advent of an identification system. It all depends on whether and when it comes, who will deal with it.

In the second part of empirical approach in the given thesis, the results of the author's study were presented, which aimed to explain the interest of potential consumers in

using biometric payments. For this purpose, a questionnaire was conducted, which was based on a versatile analysis which in turn were based on the theoretical basis and earlier empirical studies. The sample included 220 people aged 18-82 who are living in Estonia. The main respondents group was representing the younger part of the population. Nearly 60% of respondents have clearly expressed their desire for payments to be biometric. Nearly a quarter of the participants couldn´t decide, but they expressed their views on how a potential biometric payment procedure should be organized. 16,4% of questioned people said, that they wouldn´t use a biometric payment solution. Starting from the age of 55, the majority of respondents haven´t showed interest in using biometrics in their payments, as well as those who preferred cash as the primary payment method. Generally, it can be concluded that there is a high interest in biometric payments, but they could exist in parallel with existing authentication and payment methods, and 67% of respondents shared this opinion. 31% found that biometric methods in the future would replace existing methods. It is important to point out that consumers are interested in the usage of methods that are based on the both biometric authentication systems, which are biometric verification and identification systems. The interest in identification system can be assessed not only based on choices of payment option preferences, but also on the question of responsibility for the security and handling of biometric data. According to this, 41.3% of the respondents thought that it might be a governmental organization. 30.4% would trust these processes to their own bank and 28.3% would prefer to trust a separate licensed organization.

It could be concluded that initially there would be an interest in paying for your products and services biometrically, at the physical and in the online point-of-sale. Biometrical data reading could take place on a payment terminal basis, but also using a smart device. For making the payment people would prefer using their fingerprints.

The aim of the bachelor thesis was fulfilled - the interest of potential consumers in biometric payments in Estonia has been identified. There is interest in biometric payments. The set tasks for achieving the goal helped to approach the research problem in a variety of ways and also identify possible future perspectives. It is difficult to argue that the results can be transferred to the population, but gives a clear overview of the potential of the given topic. The opportunity to further develop this work is to address

this topic more in terms of the biometric identification system by assessing the potential impact on banks and authorization networks. This work is also helpful in organizing practical approaches.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Olev Gudovski,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Biomeetriliste maksete rakendusperspektiivid Eestis“,

mille juhendaja on Nadežda Ivanova,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **21.05.2018**